



**U.S. Department of Justice
Office of the Inspector General
Evaluation and Inspections Division**

The Department's and Components' Personnel Security Processes

September 2012

I -2012-003

EXECUTIVE DIGEST

INTRODUCTION

The Office of the Inspector General (OIG) examined whether the Department of Justice (Department or DOJ) and its components effectively managed the personnel security process for individuals hired into DOJ positions. We evaluated the time to complete the personnel security process for government employees, how well the Department meets the timeliness and reciprocity requirements of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) and other directives, whether certain positions take longer to process, and whether the Department can ensure that only employees with favorably adjudicated background checks have access to sensitive and National Security Information.¹

Background investigations for the Department are conducted by one of three investigative agencies – the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).² The extent of the background investigation required is determined by the type of information that individuals have access to in their work for the Department. Individuals in positions that require access to National Security Information (information classified at the Top Secret, Secret, or Confidential level) generally require more in-depth investigations than do individuals whose positions do not require access to classified information (typically termed Public Trust positions).

IRTPA requires agencies authorized to grant National Security Information clearances to complete at least 90 percent of the clearances within an average of 60 days – 40 days to complete the background investigation and 20 days to complete the adjudication determination. IRTPA's reciprocity provision mandates that agencies accept a background investigation completed by any authorized federal investigative or adjudicative agency, provided that the background investigation was favorably adjudicated, is at the right level for the position, and was completed within the past 5 years.

¹ Pub. L. No. 108-458, 118 Stat. 3638.

² Executive Order 12968 grants the Department the authority to grant, suspend, and revoke security clearances.

Investigations for Public Trust positions are not subject to the IRTPA time guideline; rather they are covered by regulations that require the adjudications to be completed and the determinations reported to OPM within 90 days. Additionally, agencies are required to apply reciprocity for Public Trust cases under 5 C.F.R. § 731.202 and Executive Order 13467, which include language similar to the IRTPA reciprocity requirement for National Security Information cases.

RESULTS IN BRIEF

The OIG found that the Department as a whole did not meet the 60-day IRTPA time guideline for processing National Security Information clearances.³ The time taken to complete the background investigation phase of the process was the primary reason for not meeting the IRTPA timeliness guideline.⁴ Table 1 summarizes the time to process completed cases.

Table 1: Time to Process Completed Security Approvals, October 1, 2009, through December 31, 2010

Investigative Agency	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	374	1,175	170	21
FBI	1,155	1,948	206	8
ATF	86	50	11	0
All DOJ (N=5,204)	1,615	3,173	387	29
Percentage	31.0%	61.0%	7.4%	0.6%

Source: OIG analysis.

We also found that approval for non-FBI attorneys took more than twice as long to complete as approvals for other personnel. Furthermore, the Department excludes most attorney positions from its timeliness reports. As a result, Department managers, and OPM, lacked

³ Not all background investigations result in granting a security clearance. For example, some individuals are granted Public Trusts and others may not be granted a security clearance until it is needed to perform a specific job.

⁴ The Justice Management Division's Security and Emergency Planning Staff (SEPS) is responsible for managing the entire security clearance process for Department personnel. However, OPM is responsible for conducting the background investigation portion of the process for some Department personnel. SEPS cannot control how long OPM takes to complete its background investigations.

information that would have alerted them to inefficiencies or delays in the non-FBI attorney clearance process.

Clearances for certain key positions in the Department such as agents, intelligence analysts, and linguists also consistently take longer than 60 days to process. As a result, these positions may go unfilled for extended periods because those persons generally cannot start work until their background adjudications have been completed. The slower processing is caused, in part, by factors such as the need to verify an individual's foreign contacts or to resolve credit issues.

The Department's time to complete Public Trust cases increased 92 percent from 99 to 190 days during the period of our review. Public Trust employees are permitted to start work under a waiver while their cases are processed. As a result, these individuals routinely work in the Department, with access to sensitive information and systems, for significant periods of time without completed background investigations and adjudications. Indeed, it took more than one year to complete the background investigations and adjudications for 3 percent of the employees in Public Trust positions, which exceeded their one year probationary periods. Accordingly, those individuals obtained permanent employment status, making it more difficult to discharge them if derogatory information was uncovered during their background investigations.

The oversight of the Department's personnel security processes by the Justice Management Division's Security and Emergency Planning Staff (SEPS) is not sufficient to identify security violations and enforce security policy. Although components track data on the status of employee background investigations, clearance levels, and reinvestigations, the tracking is inconsistent and often incomplete. Further, the field does not always have accurate information on individuals' clearance levels or the status of their investigations. The lack of information makes it difficult to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information. Finally, reciprocity data is inconsistently tracked, not reported, or reported incompletely, which made it impossible to determine whether the Department applies reciprocity consistently.

RECOMMENDATIONS

In this report, we make 13 recommendations to improve the Department's timeliness in processing background investigations and adjudications and ensure that only individuals with the appropriate clearance level have access to sensitive and classified information. These

recommendations include establishing procedures to improve the timeliness in adjudicating Public Trust cases, changing the Office of Attorney Recruitment and Management's process and staffing to improve the timeliness of attorney clearances, including timeliness data on attorney clearances in the Department's IRTPA reports, and improving SEPS's oversight of components' security clearance processes. Our recommendations also include ensuring that field offices have access to headquarters' security information and that field offices be required to know the type of clearance each employee on site holds.

TABLE OF CONTENTS

BACKGROUND 1

PURPOSE, SCOPE, AND METHODOLOGY OF THE OIG REVIEW 12

RESULTS OF THE REVIEW..... 14

 CHAPTER I: PROCESSING TIMES FOR NATIONAL SECURITY
 INFORMATION POSITIONS 14

 CHAPTER II: TIMELINESS FOR PUBLIC TRUST POSITIONS 37

 CHAPTER III: PROGRAM OVERSIGHT AND CLEARANCE
 TRACKING..... 43

CONCLUSION AND RECOMMENDATIONS 51

APPENDIX I: ACRONYMS 54

APPENDIX II: RISK LEVELS AND COST ASSOCIATED WITH
 BACKGROUND INVESTIGATION REQUIREMENTS FOR
 NATIONAL SECURITY INFORMATION AND PUBLIC TRUST
 POSITIONS..... 55

APPENDIX III: SEPS ORGANIZATION CHART 57

APPENDIX IV: INTERVIEWS 58

APPENDIX V: METHODOLOGY 61

APPENDIX VI: TIME TO COMPLETE NATIONAL SECURITY
 INFORMATION CASES PROCESSED AS PART OF THE
 FASTEST 90 PERCENT..... 65

APPENDIX VII: CASES PENDING AS OF APRIL 25, 2011 67

APPENDIX VIII: COMPLIANCE REVIEW TEAM SITE VISITS,
 FY 2010 AND FY 2011..... 68

APPENDIX IX: BUREAU OF ALCOHOL, TOBACCO, FIREARMS
 AND EXPLOSIVES RESPONSE TO DRAFT REPORT 69

APPENDIX X: OIG ANALYSIS OF THE BUREAU OF ALCOHOL,
 TOBACCO, FIREARMS AND EXPLOSIVES RESPONSE 71

APPENDIX XI: THE FEDERAL BUREAU OF PRISONS RESPONSE TO DRAFT REPORT.....	73
APPENDIX XII: OIG ANALYSIS OF THE FEDERAL BUREAU OF PRISONS RESPONSE	76
APPENDIX XIII: THE DRUG ENFORCEMENT ADMINISTRATION RESPONSE TO DRAFT REPORT	79
APPENDIX XIV: OIG ANALYSIS OF THE DRUG ENFORCEMENT ADMINISTRATION RESPONSE	81
APPENDIX XV: THE FEDERAL BUREAU OF INVESTIGATION RESPONSE TO DRAFT REPORT	83
APPENDIX XVI: OIG ANALYSIS OF THE FEDERAL BUREAU OF INVESTIGATION RESPONSE	86
APPENDIX XVII: THE U.S. MARSHALS SERVICE RESPONSE TO DRAFT REPORT	88
APPENDIX XVIII: OIG ANALYSIS OF THE U.S. MARSHALS SERVICE RESPONSE	90
APPENDIX XIX: THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE TO DRAFT REPORT.....	92
APPENDIX XX: OIG ANALYSIS OF THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE.....	98
APPENDIX XXI: THE OFFICE OF ATTORNEY RECRUITMENT AND MANAGEMENT RESPONSE TO DRAFT REPORT.....	105
APPENDIX XXII: OIG ANALYSIS OF THE OFFICE OF ATTORNEY RECRUITMENT AND MANAGEMENT RESPONSE	109

BACKGROUND

The Office of the Inspector General (OIG) is conducting a two-phase review to assess whether the Department of Justice (Department or DOJ) is effectively administering the personnel security process for employees and contractors to meet component mission and security requirements. This report discusses the first phase of the review, which focused on the time to complete the personnel security process for government employees and the Department's oversight of the components' security processes. As part of this review, we evaluated the Department's success in meeting the requirements of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) and executive branch directives.⁵ The second phase of the review will focus on the security process for contractors.

In 1995, Executive Order 12968 called for a uniform federal personnel security program for employees who will be considered for access to classified information and established security policies for protecting classified information. It also detailed individual access levels and reciprocity procedures.

IRTPA built on this Executive Order by requiring agencies that are authorized to grant National Security Information clearances to complete at least 90 percent of clearances within an average of 60 days. Those agencies are to set aside a period of not longer than 40 days to complete the investigative phase and a period of not longer than 20 days to complete the adjudicative phase of the clearance.⁶ Further, 5 C.F.R. § 732.302(b) and Executive Order 10450 require that Public Trust adjudication determinations be reported to OPM within 90-days of the completed background investigation.⁷ Table 2 summarizes the timeliness standards and regulatory guidance for National Security Information clearances and Public Trusts.

⁵ Pub. L. No. 108-458, 118 Stat. 3638.

⁶ The IRTPA guidelines establish the 60-day deadline for completing background investigations and adjudications for National Security Information clearances. These guidelines are accepted government-wide and used by ODNI to measure agency timeliness. Therefore, for the purposes of this review, the OIG used the IRTPA goal of processing the fastest 90 percent of clearances within 60 days to measure the Department's overall performance.

⁷ The language in IRTPA does not establish specific timeliness guidance for completing the security clearance process for Public Trust positions.

Table 2: Clearance Timeliness Standards and Guidance

Position Type	Background Investigation	Adjudication Determination	Reinvestigation
National Security Information	40 days based on IRTPA	20 days based on IRTPA and DOJ Order 2610.2B	Every 5 years based on DOJ Order 2610.2B
Public Trust	N/A	90 days based on 5 C.F.R. § 732.302(b), Executive Order 10450, and DOJ Order 2610.2B	Every 5 years based on DOJ Order 2610.2B

Source: OIG.

The reciprocity provision in IRTPA mandates that agencies accept a security clearance granted or accept an eligibility determination for a clearance by an authorized federal investigative or adjudicative agency provided that the clearance is not temporary or interim, and the background investigation was favorably adjudicated, was at the right security clearance level for the position, and was completed within the past 5 years.⁸

IRTPA prohibits agencies from establishing additional requirements for background investigations (except for polygraphs) without the approval of a designated agency. In 2008, Executive Order 13467 named the Office of Management and Budget (OMB) as the designated agency. OMB is responsible for managing and implementing security clearance reform throughout the federal government that pertains to adjudicating and granting clearances based on investigations.

Executive Order 13467 also mandated the use of consistent guidelines in investigations and adjudication determinations across the federal government. In addition, the Order establishes the Suitability and Security Clearance Performance Accountability Council, chaired by the Deputy Director of OMB, for the executive branch.⁹ The Council is responsible for ensuring the investigative and adjudicative processes are run properly. It monitors how agencies adhere to processing guidelines

⁸ Executive Order 12968, Executive Order 13381, and DOJ Order 2610.2B also include the requirement and any applicable exceptions for reciprocity.

⁹ The Performance Accountability Council includes representatives from OMB, the Office of Personnel Management (OPM), and the Office of the Director of National Intelligence (ODNI). DOJ is not a member of the Council, but DOJ personnel serve on the Federal Investigative Standards Working Group, which reports to the Council.

and oversees the development of tools and techniques to improve the security clearance process. As part of this function, the Council collects timeliness and reciprocity data from agencies.

National Security Information and Public Trust Positions

The type of information that individuals have access to determines the type of background investigation required for a position. Individuals in positions that require access to classified information are granted National Security Information clearances at the Top Secret, Secret, or Confidential level. A Top Secret clearance is based on a Single Scope Background Investigation (SSBI). A Secret or Confidential clearance is based on a Moderate Background Investigation (MBI), an Access National Agency Check and Inquiries (ANACI), an SSBI, or a 5-year scope Background Investigation (BI).¹⁰ IRTPA provides guidelines for such National Security Information clearances to meet.¹¹

Individuals who do not require access to classified information but who may be involved in policy making, major program responsibility, or other sensitive roles are typically considered to be in Public Trust positions. In accordance with 5 C.F.R. § 731, each DOJ position is assigned a risk level of High, Moderate, or Low based on the potential harm their actions could cause the federal government. A High Risk position requires a background investigation covering the past 5 years. A Moderate Risk position requires a Moderate Background Investigation. A Low Risk position requires a National Agency Check and Inquiries investigation. An evaluation is conducted to determine if anything in the individual's character or conduct would negatively affect the integrity or efficiency of their government service.¹²

¹⁰ An SSBI covers the past 7 years of a subject's activities and includes verification of citizenship, date and place of birth, and national agency records checks. It also includes in-person interviews of the subject and selected references. A 5-year BI is similar, except it covers only the past 5 years of a subject's activities. An MBI also covers 5 years but with mailed inquiries instead of personal interviews.

¹¹ The Office of the Director of National Intelligence (ODNI) is currently exploring the possibility of establishing a separate timeliness goals for Top Secret and Secret clearances. This is based on the premise that background investigations for Top Secret clearances are more complex and take longer to complete than investigations for Secret or Confidential clearances. However, as of the time of this report, Top Secret and Secret clearances are still subject to the IRTPA timeliness goals, as written.

¹² Section 731 of Title 5, Code of Federal Regulations establishes general guidelines for evaluating individuals in Public Trust positions. Agencies may also require candidates to meet certain agency-specific qualifications that are related to the agency's
(Cont'd.)

Timeliness in conducting background investigations and adjudications for Public Trust positions is not subject to the IRTPA time guideline. However, federal regulations require that the adjudication be completed and the determination be reported to OPM within 90 days.¹³ Further, agencies are required to apply reciprocity for Public Trust cases under 5 C.F.R. § 731.202, which prohibits agencies from making a new determination for a person who has already been determined suitable. Likewise, Executive Order 13467 states that except as otherwise authorized by law, background investigations and adjudications shall be mutually and reciprocally accepted by all agencies. Appendix II details the types of National Security Information clearances and Public Trust risk levels and the background investigation required for each position.

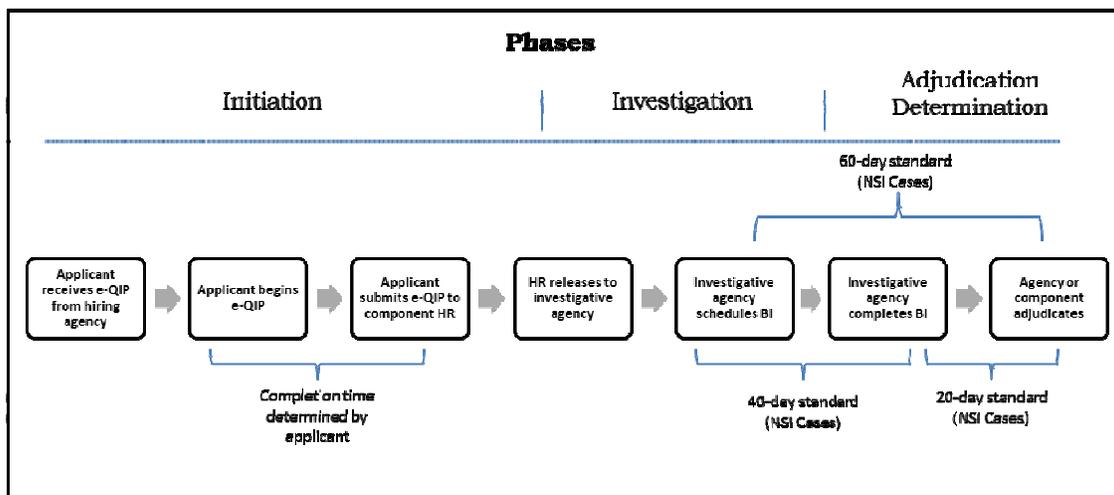
Personnel Security Process

Although the process can vary depending on the position's risk designation, in general, the personnel security process consists of a background investigation and an adjudication determination. Each component has a designated Security Programs Manager responsible for certifying that the requirements for granting security clearances are adequate and for monitoring compliance. Figure 1 depicts the typical personnel security process.

mission or key functions. For example, the Drug Enforcement Administration has a stricter drug policy, and the Bureau of Alcohol, Tobacco, Firearms and Explosives has restrictions against hiring individuals who hold a current Federal Firearms License.

¹³ 5 C.F.R. § 732.302(b) and Executive Order 10450.

Figure 1: Personnel Security Process



Abbreviations: BI = Background Investigation; e-QIP = Electronic Questionnaires for Investigations Processing system; HR = Human Resources.

Source: OIG.

To initiate the clearance process, individuals must provide background information related to their family members, residence, education, employment, finances, and criminal history. This information serves as the basis for the investigation. Since 2005, individuals have typically entered the information online using the Office of Personnel Management’s (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) system. Once the component requesting the investigation verifies the information is complete, it is sent to the agency responsible for conducting the investigation. The investigative agency conducts the investigation, which consists of verifying residence, education, employment, financial state, and criminal history. Investigators generally interview the individual, as well as family members, neighbors, and personal acquaintances.

The results of the investigation, which usually include a summary of any interviews and database checks, are sent to the adjudicating authority.¹⁴ The adjudication process examines more than a dozen variables over a sufficient period of a person’s life to determine whether the person is eligible for access to classified information or to serve in a Public

¹⁴ The results of this investigation are also used to determine if the individual is suitable to carry out the duties of a federal position with integrity, efficiency, and effectiveness. This suitability determination is often conducted concurrently with the security adjudication.

Trust position. Available information about a person's past and present, favorable and unfavorable, is used to make determination decisions.

Employees holding a security clearance who have been employed in their jobs for certain periods of time are subject to a reinvestigation to verify that they should still have access to classified National Security Information. A reinvestigation is required once every 5 years for individuals possessing a Top Secret clearance, once every 10 years for those with a Secret clearance, and once every 15 years for those with a Confidential clearance.¹⁵ Federal agencies may impose additional requirements to expand the number of individuals subject to reinvestigation or to require more frequent reinvestigations, and the Department has decided to require both Public Trust employees and those with National Security Information clearances to be reinvestigated once every 5 years. The hiring agency or the component headquarters usually monitors expiration dates.

Authorities to Conduct Background Investigations and Adjudications

The authorities to conduct background investigations and make adjudication decisions for Department employees vary from component to component.

Background investigations for Department employees are conducted by one of three authorized investigative entities, one of them outside the Department, OPM, and two of them inside the Department, the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). All three agencies have authority to complete background investigations for both National Security Information and Public Trust positions. Regardless of which agency performs an investigation, all background investigations have to meet the same government-wide standards.¹⁶ Agencies' processes differ slightly as will be discussed in the sections below.

The Justice Management Division's (JMD) Security and Emergency Planning Staff (SEPS) is authorized to make adjudication determinations for both Public Trust positions and National Security Information

¹⁵ 50 U.S.C. § 435b(A)(7).

¹⁶ Executive Order 12968 and Executive Order 13467.

positions.¹⁷ SEPS further delegated some of this adjudication authority to ATF, the Federal Bureau of Prisons (BOP), the Drug Enforcement Administration (DEA), the FBI, and the U.S. Marshals Service (USMS) so these agencies could make adjudication determinations for their own employees. SEPS makes the adjudication determinations for the remainder of the Department.

Table 3 details each component’s authority and shows which component is responsible for conducting investigations and adjudications.

Table 3: Background Investigation and Adjudication Authority

Component	Who Has Authority to Conduct Background Investigations for:		Who Has Authority to Adjudicate Security Clearances for:	
	Employees (non-attorneys)	Attorneys	Employees (non-attorneys)	Attorneys
ATF	ATF	FBI	ATF	SEPS
BOP	OPM	FBI	BOP	SEPS
DEA	OPM	FBI	DEA	SEPS
USMS	OPM	FBI	USMS	SEPS
FBI	FBI	FBI	FBI	FBI
All Other Components	OPM	FBI	SEPS	SEPS

Source: OIG.

DOJ Personnel Security Process

SEPS is the primary office responsible for developing, implementing, and ensuring compliance with security policy throughout the Department. Within SEPS, the Personnel Security Group and the Office of Information Safeguards and Security Oversight’s Compliance Review Team handle policy and oversight specific to the Department’s security clearance process.

The Personnel Security Group has two sections. The Policy, Oversight, and Training Section develops Department-wide personnel security policy and training, while the Operations Section reviews and adjudicates background investigations for government employees and contractors. Within the Office

¹⁷ 28 C.F.R. § 17.11(c) and Executive Order 12968 grant the Department the authority to grant, suspend, and revoke security clearances and to delegate its authority to the components. In 5 C.F.R. § 731, OPM delegated agencies the authority to adjudicate Public Trust positions.

of Information Safeguards and Security Oversight, the Compliance Review Team conducts both scheduled and unscheduled on-site security reviews of DOJ components. Appendix III details SEPS's organizational structure.

SEPS also manages the Justice Security Tracking and Adjudication Record System (JSTARS), a web-based personnel security processing application that tracks background investigations, adjudications, reinvestigations, and reciprocity requests across the Department. Select components have direct access to JSTARS, while other components receive monthly update reports from SEPS. The majority of components moved their data to JSTARS by the end of 2011. The remaining components, except the FBI, are scheduled to move their data to JSTARS in 2012. The FBI stores its personnel security data in a classified system that is not compatible with JSTARS. As a result, the FBI will report its personnel security data to JSTARS, but will continue to use internal FBI systems to track personnel security data.

The following sections describe the three primary personnel security processes used within the Department.

Background Investigations Completed by OPM

Many Department components, including JMD and the OIG, rely on OPM's Federal Investigative Services (FIS) to conduct background investigations. FIS, in fact, conducts the background investigations for most of the Department's employees, except for attorneys, political appointees, and employees of the FBI and ATF.¹⁸ FIS initiates the background investigation process after an agency submits an individual's completed security application via e-QIP, along with a set of fingerprint cards and signed release forms authorizing FIS to conduct an investigation. FIS reviews the e-QIP application to ensure it is complete and includes all the required documentation.¹⁹ Once FIS receives all the

¹⁸ OMB delegated authority to OPM's FIS to conduct background investigations for the federal government (Executive Order 10450 on Security Requirements for Government Employment and Executive Order 12968 on Access to Classified Information). FIS provides investigative services for 126 federal agencies and conducts approximately 2.2 million background investigations a year. It conducts high-level investigations for access to National Security Information as well as the lower-level checks required under the Homeland Security Presidential Directive 12 (HSPD-12) for anyone accessing federal space or information systems.

¹⁹ If information is missing, OPM's FIS returns the application to the agency. According to OPM, only 6 percent of the application forms submitted through e-QIP are returned due to missing information. OPM believed the return rate for forms that are submitted on paper is around 55 percent.

required information, the e-QIP system validates the forms and an investigation is scheduled within 24 hours. OPM uses contractors to conduct the investigation. When the investigation is completed, FIS releases the information to the agency that requested the investigation.

The completed investigation is forwarded to the appropriate adjudicating authority for a decision. According to federal regulations, the agency must report its adjudicative determinations to OPM within 90 days of receiving the completed investigation.²⁰

Background Investigations Completed by the FBI

The FBI conducts the background investigations for its own employees and also makes the adjudication determinations.²¹ The FBI's Security Division handles personnel security for FBI employees.²²

An FBI background investigation includes completing and submitting security forms in e-QIP, a urinalysis examination, a personnel security interview, and a polygraph examination. All FBI applicants must pass a polygraph examination as part of agency-specific qualifications. Certain positions may also require the applicant to pass a physical or medical examination.

The field office reviews the forms for completeness, notes any derogatory information, and forwards the forms to the appropriate Security Division unit. The unit assigns a case manager who is responsible for monitoring the file throughout the security clearance process. The case manager initiates the background investigation, schedules the interview leads for the contractor investigators or an FBI agent assigned to the

²⁰ 5 C.F.R. § 732.302(b) and Executive Order 10450.

²¹ The FBI's authority is derived from 5 U.S.C. §§ 3301 and 9101 and from Executive Order 10450 on Security Requirements for Government Employment and Executive Order 12968 on Access to Classified Information.

²² Within the Security Division, separate staffs handle different types of employees. For example, two Professional Staff Clearance Units are responsible for all professional staff and specialty hires, such as intelligence analysts, surveillance specialists, FBI attorneys and interns. The Special Clearance Unit (SCU) conducts background investigations for FBI special agents, while the Special Inquiry and General Background Investigations Unit (SIGBIU) conducts background investigations for non-FBI attorneys. Each staff operates independently of the others and has an intake function, an investigative function, an adjudicative function, and a process function.

investigation, and makes the final adjudication determination.²³ All FBI employees are cleared at the Top Secret level, and there are no Public Trust positions in the FBI.²⁴

Background Investigations Completed by ATF

ATF conducts the background investigations for its employees and makes the adjudication determinations under authority delegated to it by OPM. ATF's Personnel Security Branch, located at headquarters, centrally manages the security clearance process. ATF's field offices have very little involvement. The Personnel Security Branch initiates its security process for a new employee in response to a request from the Office of Human Resources and Professional Development. The branch reviews the request to ensure the applicant meets ATF's agency-specific qualifications.²⁵ All ATF positions are considered to be National Security Information positions, and most ATF employees require a Top Secret clearance. ATF does not have any Public Trust positions.

The Personnel Security Branch is also responsible for scheduling the background investigation for the applicant. ATF uses either independent contract field agents or OPM's FIS to complete background investigations. Most are done by ATF contract employees. The contract field agents must follow a Special Investigator Manual modeled on OPM's investigations manual. The Personnel Security Branch monitors the field agents' investigations to ensure the agents are conducting all the necessary field work and meeting OPM's standards.

²³ The FBI's Background Investigation Contract Service (BICS) Unit is responsible for managing approximately 1,100 FBI contractors that are tasked with conducting investigative leads. FBI employees working within the BICS unit review and approve the completed leads before providing the results to the requesting unit within the Security Division. However, FBI special agents and other professional support staff may assist with certain cases, such as a political appointee, or to run local checks.

²⁴ The FBI also conducts background investigations for the Department's non-career Senior Executive Service appointees, Schedule C appointees, attorneys, law clerks, and all positions in the Office of the Attorney General and the Office of the Deputy Attorney General in accordance with DOJ Order 2610.2B, Employment Security Order, Section 12. These investigations are handled by SIGBIU. For these cases, the requesting agency or component is responsible for collecting the individual's security forms and reviewing them for completeness. The agency or component submits these forms to the SIGBIU, which conducts the background investigation and returns the investigation result to the adjudicating agency.

²⁵ ATF's agency-specific qualifications include a stricter drug policy and restrictions against hiring individuals involved in alcohol-related businesses or who hold a current Federal Firearms License.

The contract field agents can complete investigations for approximately half the cost of FIS. Using contract field agents also allows ATF to cancel investigations at any time during the process and pay only for the portion that has been completed, rather than paying the full cost as FIS requires. ATF does sometimes use FIS to conduct lower-level background investigations that do not require field work.

Once an investigation is completed, a Personnel Security Branch adjudicator reviews the file and summarizes any issues in a report. The files and reports are reviewed by the Branch Chief, who can make a determination on whether to approve the individual for hire.

Prior OIG and Government Accountability Office Reports

Prior OIG reports found that certain Department components did not have effective personnel security processes, which resulted in untimely background investigations and adjudications, personnel having unauthorized access to sensitive Department data and facilities, and other problems with the personnel security process. In addition, prior Government Accountability Office (GAO) reports focused on reforms to the government security clearance process, removing the Department of Defense personnel security clearance process from the GAO's list of high-risk designation areas, and the need for OPM to improve transparency in its pricing and to seek cost savings.²⁶

²⁶ The prior OIG reports were *Implementation of the Contractor Personnel Security Program in Selected Offices, Boards, and Divisions*, Evaluation and Inspections Report I-01-004 (March 2001); *Review of the Security and Emergency Planning Staff's Management of Background Investigations*, Evaluation and Inspections Report I-2005-010 (September 2005); *United States Marshals Service's Use of Independent Contractors as Guards*, Audit Report 05-24 (May 2005); *The Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 05-20 (May 2005); *Background Investigations Conducted by the United States Marshals Service*, Evaluation and Inspections Report I-2005-002 (February 2005); *Follow-up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 07-30 (April 2007); *The Federal Bureau of Investigation's Foreign Language Translation Program*, Audit Report 10-02 (October 2009); and *Audit of the United States Marshals Service's Oversight of its Judicial Facilities Security Program*, Audit Report 11-02 (November 2010).

The prior GAO reports were *Personnel Security Clearances: Overall Progress Has Been Made to Reform the Governmentwide Security Clearance Process*, GAO-11-232T (December 1, 2010); *High-Risk Series: An Update*, GAO-11-278 (February 2011); and *Background Investigations: Office of Personnel Management Needs Improve Transparency of Its Pricing and Seek Cost Savings*, GAO-12-197 (February 2012).

PURPOSE, SCOPE, AND METHODOLOGY OF THE OIG REVIEW

The purpose of the OIG's review is to assess whether the Department is effectively administering the personnel security process for employees and contractors to meet component mission and security requirements. This review consists of two phases. The first phase focused on government employees, including the time it takes to complete background investigations and adjudications and the Department's success in meeting IRTPA's timeliness and reciprocity requirements. The second phase will focus on the specific issues with the contractor personnel security program and will be covered in a separate, subsequent report.

The objectives of the first phase of the review were to assess:

- whether the Department and its components are meeting the timeliness and reciprocity requirements of IRTPA for National Security Information cases;
- whether the Department and its components are timely in processing personnel security cases;
- whether clearances for specific positions take longer to process;
- whether the Department and its components provide effective controls over the personnel security process;
- whether the Department provides sufficient oversight of the components' personnel security processes; and
- whether the Department ensures that personnel with access to sensitive or classified information possess the appropriate background investigation.

This review examined the Department's timeliness for the end-to-end process, regardless of whether the investigative agency was part of the Department (the FBI and ATF) or outside the Department (OPM).

Department components we reviewed included ATF, the Antitrust Division, the Environment and Natural Resources Division, the BOP, the Civil Division, the Civil Rights Division, the Criminal Division, the DEA, the Executive Office for United States Attorneys (EOUSA), the FBI, JMD, the Office of Attorney Recruitment and Management (OARM), the Office of Justice Programs, the United States Attorneys' Offices (USAO), and USMS. Our review included interviews, data analysis, document reviews, and site visits.

The review covered the period since the enactment of IRTPA to the last full fiscal year, specifically fiscal year (FY) 2005 through the first

quarter of FY 2011. We conducted our fieldwork from March 2011 through July 2011.

Interviews

We interviewed a total of 106 officials and staff members at the various components' headquarters and field offices. We also interviewed Government Accountability Office personnel to discuss its previous reviews as well as OPM personnel regarding investigation and clearance procedures. The interviewees are listed in Appendix IV.

Data Analyses and Document Reviews

We analyzed component data on security and personnel information from FY 2010 through the first quarter of FY 2011 (October 1, 2009, through December 31, 2010). We chose this period based on when agencies were required to meet the current IRTPA guideline. The data included when the background investigation was initiated, when the background investigation was completed, when the adjudication determination was made, the risk or sensitivity level, and the job position. We also reviewed relevant laws, regulations, policies, procedures, internal reviews, and a sampling of security files for completed background investigations. See Appendix V for a detailed description of the OIG's methodology used for each analysis.

Site Visits

We conducted site visits to 14 ATF and FBI field offices, USMS and USAO district offices, DEA division offices, and BOP confinement facilities in Los Angeles and Atlanta. We also visited JMD and each law enforcement component's headquarters, as well as the Civil Division, the Civil Rights Division, the Criminal Division, EOUSA, and OARM.

RESULTS OF THE REVIEW

CHAPTER I: PROCESSING TIMES FOR NATIONAL SECURITY INFORMATION POSITIONS

The Department as a whole and many of its components did not meet the 60-day IRTPA time guideline for processing National Security Information clearances during the period of our review. In addition, the Department excludes most attorney positions from its timeliness reports. As a result, Department managers have lacked information that would have alerted them that it takes significantly longer to complete clearances for non-FBI attorneys than for other personnel. Clearances for certain other key positions in the Department also consistently take longer than 60 days to process, and as a result, these positions may go unfilled for extended periods. The slower processing is caused, in part, by factors such as the need to verify an individual's foreign contacts or to resolve credit issues, but is also caused by inefficiencies in the Department's process.

The Department as a whole and many of its components did not meet the 60-day IRTPA time guideline for processing National Security Information clearances, primarily because of the time taken to complete background investigations.

Taken as a whole, it took the Department approximately 81 days to complete security clearances for the fastest 90 percent of National Security Information cases.²⁷ This was primarily due to the length of time it took to complete a background investigation.²⁸ The background investigation phase alone averaged 66 days to complete, exceeding the

²⁷ These numbers represent the overall averages for the fastest 90 percent of cases for the entire Department, rather than the average of 100 percent of the total investigations completed. We will discuss timeliness for each investigative agency – OPM, the FBI, and ATF – later in this chapter.

²⁸ SEPS is responsible for managing the entire security clearance process for Department personnel. However, OPM conducts the background investigation portion of the clearance process for some Department personnel. SEPS cannot control how long OPM takes to complete its background investigations.

IRTPA 40-day timeliness guideline by 26 days. The Department met the 20-day guideline for adjudications, averaging 15 days for that phase of the process.

None of the three entities conducting background investigations for the Department – OPM, the FBI, and ATF – met IRTPA’s 40-day timeliness guideline. ATF background investigations came closest to meeting the guideline, averaging 45 days, while OPM averaged 61, and the FBI averaged 69 days.²⁹

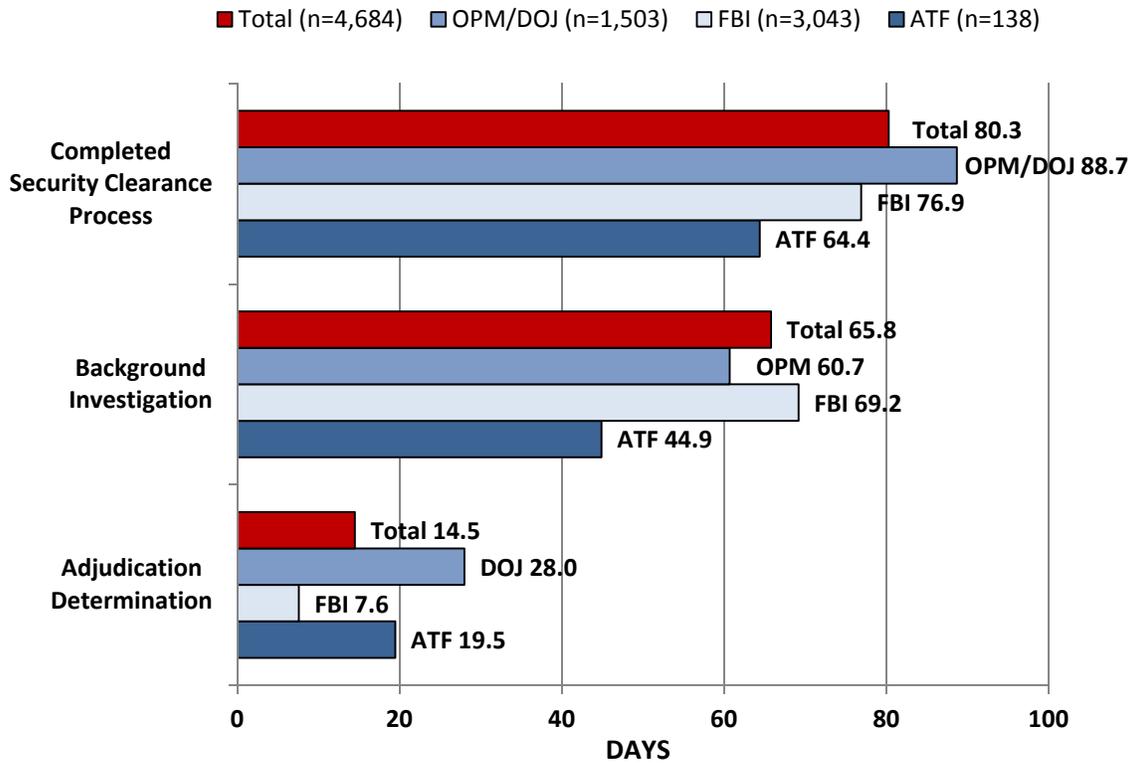
ATF and the FBI completed adjudications within the 20-day IRTPA timeliness guideline, with ATF averaging 20 days and the FBI averaging only 8 days. The rest of the Department exceeded the guideline, on average by 8 days.³⁰ In terms of total time taken, ATF processed National Security Information clearances in an average of 64 days, while the FBI averaged 77 days, and OPM averaged 89 days (Figure 2).³¹

²⁹ The OIG also analyzed the slowest 10 percent of all newly hired employee cases to identify any factors that contributed to additional processing time. However, this analysis did not reveal trends or patterns that might indicate why these cases took longer to process.

³⁰ Cases referred to as “OPM/DOJ” in Figures 2 through 5 are those in which the background investigations were conducted by OPM and the adjudication determinations were completed by one of the Department’s components.

³¹ These numbers were calculated using the timeliness data the Department currently reports to ODNI. Attorneys (except for FBI attorneys) were not included in this analysis because timeliness data for them is not currently reported to ODNI. A separate analysis of timeliness for attorney clearances is discussed further in Chapter I of this report.

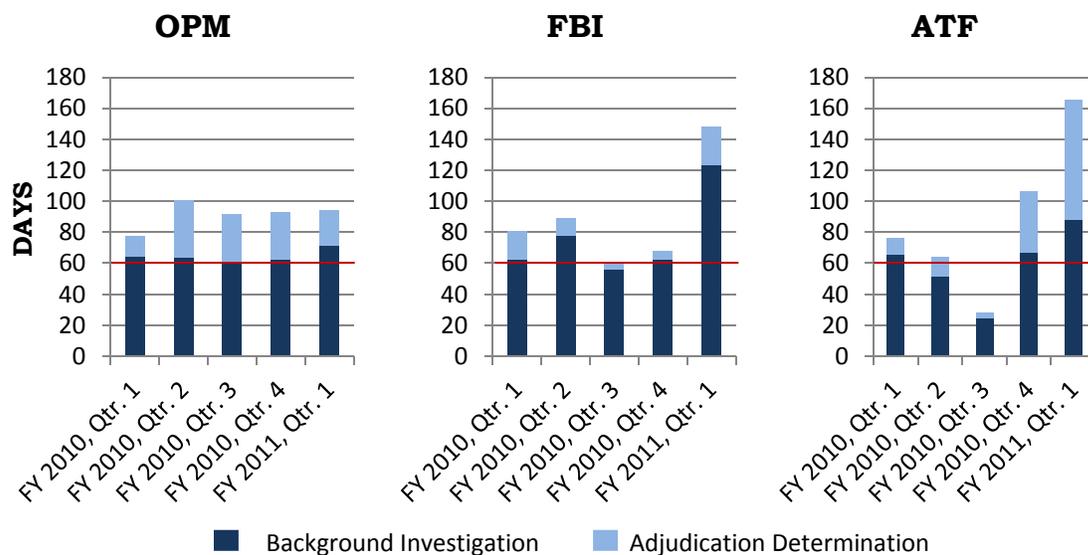
Figure 2: Average Timeliness by Investigative Agency, October 1, 2009, through December 31, 2010



Source: OIG analysis.

The OIG further analyzed, by investigative agency, the average time of the fastest 90 percent of National Security Information cases to complete background investigations and adjudications over 5 quarters of data (Figure 3).

Figure 3: Comparison of Security Approvals by Investigative Agency, October 1, 2009, through December 31, 2010

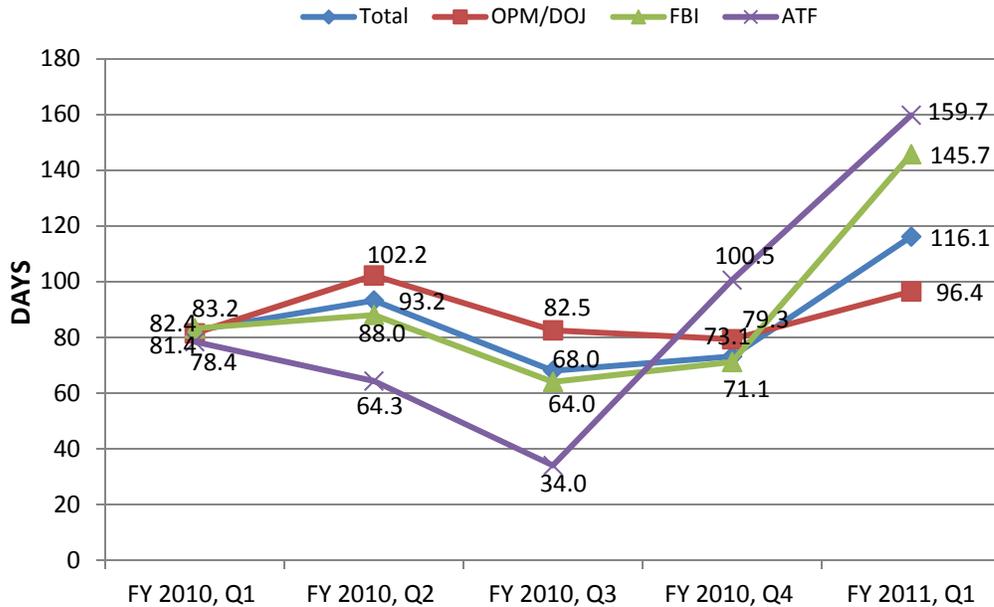


Source: OIG analysis.

As the data shows, background investigations completed by OPM ranged from 52 to 73 days over the 5 quarters we examined. Likewise, during that period the Department’s adjudication times for OPM’s investigations was between 20 and 38 days. However, in general, the background investigation rather than the adjudication determination caused the Department to exceed the 60-day IRTPA guideline. Similarly, FBI background investigations consistently exceeded the 40-day IRTPA guideline, increasing the FBI’s average processing times. Although ATF had the fastest overall investigation times, ATF’s completion time varied significantly within each quarter. During the first quarter of FY 2011, ATF adjudications took longer to complete than the background investigation, and the entire process averaged 160 days in that quarter.

Overall, the Department’s time to complete a security approval improved slightly between the first and fourth quarters of FY 2010, from 82 days to 73 days. However, its time increased to 116 days in the first quarter of FY 2011. This was primarily due to the fact that ATF and the FBI took significantly longer to complete cases during this time period (Figure 4).

Figure 4: Timeliness of Completed Security Approvals, October 1, 2009, through December 31, 2010



Cases Processed by Quarter				
	OPM/DOJ	FBI	ATF	Total (all DOJ)
FY 2010, Qtr 1	262	444	22	728
FY 2010, Qtr 2	397	508	32	937
FY 2010, Qtr 3	338	740	58	1,136
FY 2010, Qtr 4	309	1,233	17	1,559
FY 2011, Qtr 1	197	118	9	324
Total (all quarters)	1,503	3,043	138	4,684

Source: OIG analysis.

Both ATF and the FBI completed significantly fewer cases in the first quarter of FY 2011. However, the time to complete these cases increased. In the first quarter of FY 2011, the FBI completed 118 clearances in an average of 146 days. In the previous quarter, the FBI completed more than 10 times that number in half the time (71 days). An FBI Security Division official stated that at the end of every fiscal year, the division reviews all pending cases and prioritizes them to meet the FBI's hiring goals. Cases that can be favorably adjudicated more quickly are completed in the fourth quarter of the fiscal year, while cases

that may take additional time are completed in the first quarter of the following year.³²

In the first quarter of FY 2011, ATF completed nine cases in an average of 160 days. In the previous quarter, ATF completed nearly twice that number, but its average time was 101 days (about a third faster). ATF security personnel stated that because they were operating under a Continuing Resolution in the first quarter of FY 2011, they did not have sufficient funding to pay for new investigations or complete pending investigations.

The OIG's analysis determined that 116 (98 percent) of the FBI cases and all of the ATF cases completed in the first quarter of FY 2011 took more than 60 days to complete. The 116 FBI cases ranged between 75 and 211 days, and the ATF cases ranged from 90 to 208 days.³³ In contrast, during the fourth quarter of FY 2010, 71 percent of ATF cases and 57 percent of FBI cases took more than 60 days to complete. As a result, both ATF's and the FBI's average processing times increased.

The majority of security approvals were completed within 6 months.

We found that the Department failed to complete security approvals within the established IRTPA timeframes for 69 percent of cases.³⁴ The majority (61 percent) of cases were completed between 61 and 180 days (Table 4). Only 8 percent of completed cases took more than 180 days to complete, and less than 1 percent took more than a year to complete.³⁵

³² The OIG was not able to verify if this was a trend because data from the fourth quarter of FY 2009 was outside of the scope of this review and the requirement to complete 90 percent of clearances in an average of 60 days was not implemented until the first quarter of FY 2010. Prior to this date, IRTPA required only 80 percent of clearances to be completed in an average of 120 days.

³³ The OIG also determined that neither the FBI nor ATF initiated any new investigations during the first quarter of FY 2011 (October 1, 2010, through December 31, 2010). Instead, they completed cases that had been in process from prior quarters.

³⁴ For this portion of our analysis, the OIG analyzed 100 percent of National Security Information cases.

³⁵ See Appendix VI for a breakdown of National Security Information cases by quarter and by investigative agency.

**Table 4: Time to Process Completed Security Approvals,
October 1, 2009, through December 31, 2010**

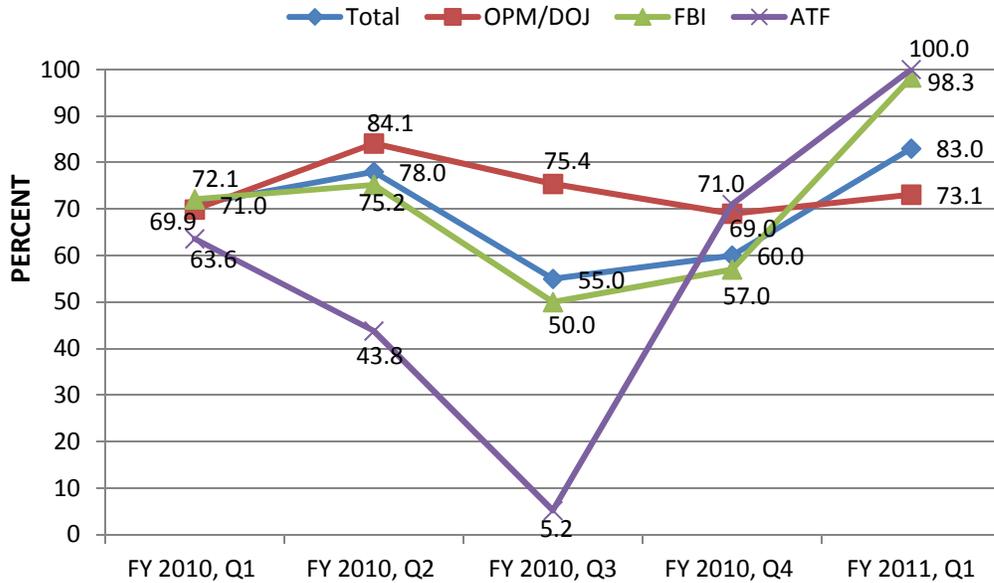
Investigative Agency	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	374	1,175	170	21
FBI	1,155	1,948	206	8
ATF	86	50	11	0
All DOJ (N=5,204)	1,615	3,173	387	29
Percentage	31.0%	61.0%	7.4%	0.6%

Source: OIG analysis.

The OIG also analyzed the Department’s caseload to determine what percentage of cases took more than 60 days to complete in each quarter (Figure 5).³⁶

³⁶ This analysis was conducted for the fastest 90 percent of cases to show how cases that took more than 60 days affected the Department’s timeliness in meeting the IRTPA standard.

Figure 5: Security Approvals Exceeding Time Guidelines, as a Percentage of Caseload, October 1, 2009, through December 31, 2010



Source: OIG analysis.

For the period we analyzed, 55 percent to 83 percent (an average of 69 percent) of the Department’s caseload consisted of cases older than 60 days. For example, in the fourth quarter of FY 2010, 60 percent of the cases took more than 60 days to complete, and the Department completed cases in an average of 73 days. In the first quarter of FY 2011, 83 percent of the Department’s cases exceeded 60 days, and the time to complete a case increased to 116 days.³⁷

Cases Pending Over 60 Days

Our data set for this review included 5,434 National Security Information clearance cases that fell within the project’s scope.³⁸ Of these, 1,073 were open and pending at the start of the review period

³⁷ Data on the average number of days taken is derived from Figure 4 in this report. Data on the percentage of cases that took more than 60 days to complete is derived from Figure 5 above.

³⁸ The OIG requested data from the components on all cases that were initiated on or before December 31, 2010, and were either completed during the time period covered by our review (October 1, 2009, through December 31, 2010) or were still missing an adjudication determination at the end of the review period.

(October 1, 2009). At the end of the review period, 230 cases were open and were still pending either a background investigation or adjudication determination.³⁹

Of those pending 230 cases, 221 had been pending for more than 60 days, and, of those, 87 had been pending for more than a year. Table 5 shows the days in process for these pending cases.⁴⁰

Table 5: Pending Cases

Status of Case	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
Pending Investigation	3	19	22	12
Pending Adjudication	6	32	61	75
All DOJ (N=230)	9	51	83	87

Source: OIG analysis.

The Department takes significantly longer to complete clearances for non-FBI attorneys than for other personnel and does not include all attorney data in its IRTPA timeliness reports.

During discussions with the FBI, SEPS, and OARM, and through a review of the Department’s data, the OIG discovered that data on the majority of attorney clearances is not included in the Department’s IRTPA timeliness reports to OPM. SEPS is responsible for working with OPM to ensure all of the Department’s data, including attorney data is available for inclusion in performance reports. The Office of the Director of National Intelligence (ODNI) uses this data to provide the Department with quarterly feedback reports detailing its performance in meeting IRTPA timeliness goals. However, we found that only data on FBI attorneys was being reported to OPM, which amounted to 11 percent (28 of 262) of the Department’s attorney clearances processed during the period we reviewed. As a result, Department managers were not aware

³⁹ The OIG confirmed with the components that these cases were considered to be active or still pending as of April 25, 2011, which was the date components were required to submit their data. However, based on the data, we could not determine whether individual cases were pending because of issues in the investigative process or because they had not yet been reviewed.

⁴⁰ See Appendix VII for a breakdown of pending cases by quarter and by investigative agency. The FBI was not able to provide data for pending cases that were initiated before May 1, 2010.

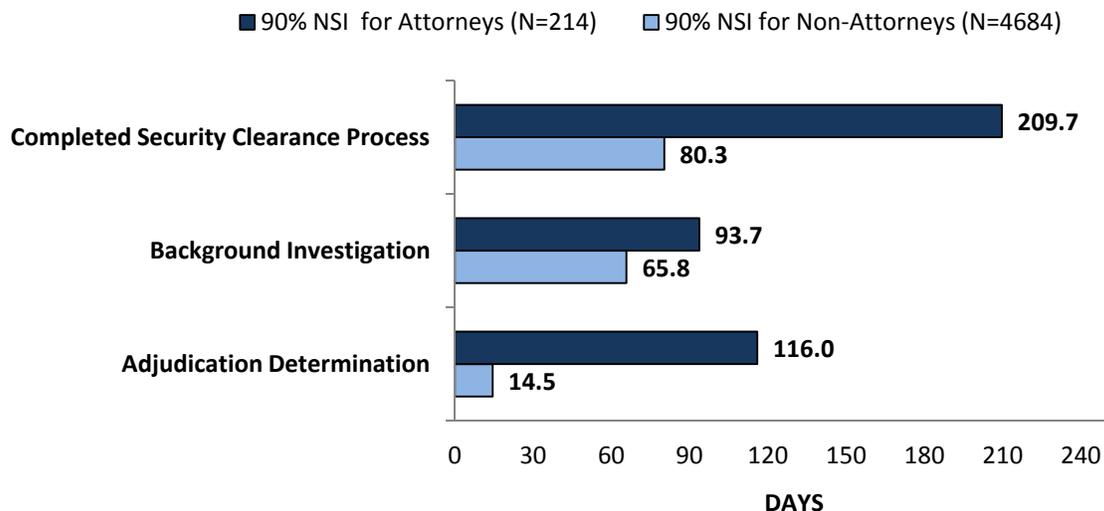
that it takes significantly longer to complete clearances for non-FBI attorneys than for other personnel.

The OIG analyzed the Department's reported data and determined that attorneys accounted for 5 percent of the Department's completed clearances during the time period of this review. Figure 6 shows the Department's average time in completing the fastest 90 percent of clearances for attorneys and other personnel. The overall clearance process for the Department's attorneys took more than twice as long (210 days) to complete compared with that for other personnel (81 days). Background investigations, on average, took 94 days for attorneys, compared with 67 days for other personnel.⁴¹ Adjudication determinations for the Department's attorneys took almost eight times longer (116 days) to complete compared with determinations for other personnel (15 days). However, we concluded that omitting attorney data did not significantly affect the Department's overall reported timeliness in completing security clearances.⁴²

⁴¹ The FBI conducts background investigations for all of the Department's attorneys. However, it conducts adjudications only for FBI attorneys, while SEPS conducts adjudications for the rest of the Department's attorneys.

⁴² Our analysis showed that if attorneys had been included in the Department's IRTPA timeliness report, the reported time to complete the fastest 90 percent of clearances would have increased from approximately 81 days to 83 days during the period of our review. Including the Department's attorneys would have had minimal impact on reported timeliness because most cases would have been among the 10 percent excluded when calculating the fastest 90 percent of clearances processed under the IRTPA standard.

Figure 6: Timeliness in Completing National Security Information Cases for Attorneys and Non-Attorneys, October 1, 2009, through December 31, 2010



Source: OIG analysis.

In examining the process, we found that when the FBI completes an attorney’s investigation, it sends the investigation results, along with the investigation dates, to OARM.⁴³ OARM completes a suitability determination based on the completed FBI background investigation and then sends the results of its determination and the FBI investigation to SEPS, which makes a security adjudication determination.⁴⁴

SEPS uploads the results of these adjudication determinations and the dates of the investigations into JSTARS. JSTARS is used to report timeliness data for the Department’s non-attorney hires to OPM. However, attorney data, along with the time taken to complete each investigation and adjudication, is not included in the data reported to OPM.

⁴³ In accordance with DOJ Order 2610.2B, Section 7, OARM must promptly make suitability determinations for all Department attorneys. This suitability determination addresses an individual’s ability to carry out the duties of their federal position with integrity, efficiency, and effectiveness. The suitability determination is based on the completed background investigation. However, it is not subject to IRTPA guidelines and, as a result, fell outside the scope of our review.

⁴⁴ The process differs slightly for FBI attorneys. The FBI completes the security adjudications for FBI attorneys before sending them forward to OARM for suitability reviews. SEPS is not involved in this process.

Personnel at ODNI, OPM, and SEPS management confirmed to the OIG that attorney security clearances are subject to the IRTPA guidelines and data on processing these clearances should be reported to OPM.⁴⁵ Further, the FBI, OARM, and SEPS told the OIG that they have discussed at various times the issue of reporting attorney data. OPM and SEPS stated that there were interface problems with the various systems used to report the data and they were working toward implementing a manual process to ensure that attorney data is included. However, as of December 31, 2011, no solutions had been implemented and the data was still being excluded from the Department's timeliness data. SEPS security staff stated that after IRTPA was implemented, the issue "fell through the crack."

Security approvals for attorneys consistently took longer than 60 days to complete.

Between October 1, 2009, and December 31, 2010, security approvals for attorneys consistently exceeded the 60-day guideline. Background investigations for attorney cases took between 16 and 356 days, averaging 99 days to complete. Adjudications took from 2 to 693 days, and averaged 135 days to complete.

Department attorneys, except for those employed by the National Security Division and the FBI, typically start work under time-limited appointments while their background investigations are being completed.⁴⁶ According to OARM, such appointments do not exceed 18 months.⁴⁷ During this time, the FBI conducts background

⁴⁵ ODNI is responsible for overseeing the intelligence community, including issuing guidance and policies regarding National Security Information. ODNI also measures agencies' success in meeting the IRTPA guidelines.

⁴⁶ Attorneys working for the National Security Division and the FBI are prohibited from starting work under a time-limited appointment and must wait until they have an adjudicated background investigation to start work. Unlike other components, the FBI manages the background investigation and adjudication determination process for its attorneys and their cases go through OARM only for attorney suitability determinations. Because this review focused on the end-to-end process for security clearances, we excluded FBI attorneys from this analysis. Instead, we included them in the discussion of FBI employees.

⁴⁷ According to 5 U.S.C. § 8906(a)(1), 5 C.F.R. § 213.104(a)(1), and the OPM Federal Employee Health Benefits (FEHB) Handbook, to be eligible for FEHB coverage, attorneys who have not yet passed their background investigations must be appointed to time-limited terms in excess of 1 year. If they are not, the attorneys will be viewed as "temporary" employees and ineligible for FEHB coverage until they have completed 1 year of current continuous employment. To ensure the availability of health benefits

(Cont'd.)

investigations to enable these attorneys to be eligible for National Security Information clearances.⁴⁸ Once an attorney's background investigation is complete, OARM conducts an internal review of agency-specific requirements and then sends the investigation to SEPS's Personnel Security Group for the security adjudication.⁴⁹ If the Personnel Security Group makes a favorable adjudication, the attorney receives an appointment for a permanent position and is eligible to hold a security clearance.⁵⁰

The OIG calculated the average time to complete a security approval for a new attorney during the period from October 1, 2009, through December 31, 2010. Overall, the length of time decreased from 406 to 188 days, an improvement of 218 days between the first quarter of FY 2010 and the first quarter of FY 2011 (see Figure 7). This was primarily due to a decrease in the amount of time it took to complete adjudication determinations. The time to complete adjudications improved by 68 percent between the first quarter of FY 2010 and the first quarter of FY 2011, while the time to complete investigations improved by only 17 percent. Despite the improvement, attorney security approvals still exceeded the 60-day guideline in all quarters analyzed. Background investigations took between 3 and 4 months (93 to 116 days) to complete, exceeding the 40-day guideline. However, they were completed much faster than the 14 months taken in 2007. Adjudications also consistently exceeded the 20-day guideline for this phase of the process. In fact, in 4 of the 5 quarters, the adjudication

for incoming attorneys, OARM originally set the time-limited appointments to a period of 14 months. OARM subsequently expanded this period to 18 months due to delays in FBI background investigations and the resulting need to extend attorneys' appointments to keep them on board while the investigations were completed. Louis DeFalaise, Director, Office of Attorney Recruitment and Management, Memorandum to Executive Officers of Offices, Boards and Divisions, Revised Memoranda of Agreement for Attorneys and Law Clerks, January 4, 2007. Although OARM used the term "temporary" instead of "time-limited" in the Revised Memoranda, it has confirmed that its use of the term "temporary" was not consistent with the use of the term as defined in 5 C.F.R. § 213.104(a)(1) and that the attorneys are not appointed on a temporary basis.

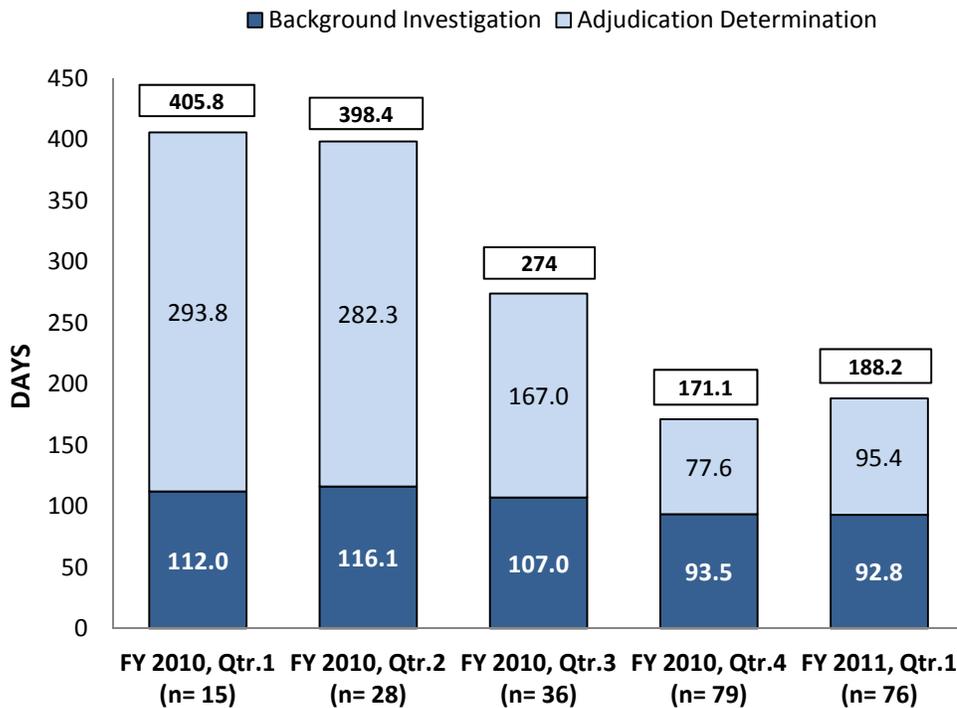
⁴⁸ Although the SSBI makes attorneys eligible for security clearances, they do not automatically receive one unless it is required for their positions.

⁴⁹ OARM processes all attorney hires in the Department. However, the FBI manages the security clearance process for its own attorneys and includes data on FBI attorneys in its IRTPA timeliness reports.

⁵⁰ Attorneys are eligible for a permanent appointment as soon as their background investigation is favorably adjudicated. After an attorney receives a permanent appointment, the attorney must serve a 2-year probationary period.

determination took longer than the background investigation – averaging between 4 and 10 months to complete (95 to 294 days).

Figure 7: Timeliness in Completing Security Approvals for Attorneys, October 1, 2009, through December 31, 2010



Source: OIG analysis.

On average, security approvals for attorneys were completed before the expiration of the 18-month time-limited appointment, with most approvals completed in less than a year during the last 2 quarters of FY 2010 and the first quarter of FY 2011. This indicates that the 18-month appointment may no longer be necessary and that the length of the appointments could be reduced to either the pre-2007 14-month period or to a shorter time period that more accurately represents the length of the clearance process.

The OIG examined the security files for the attorney cases that took the longest to complete to determine if issues such as foreign connections or credit affected the length of the security clearance process. One case took 589 days to complete, with 62 days to complete the background investigation and 527 days to complete the adjudication. The other case took 606 days to complete, with 113 days for the background investigation and 493 days for the adjudication. Neither case had significant problems or derogatory issues that needed to be

resolved. However, the case documentation showed that once the investigations were completed, OARM held the files for 6 to 9 months before sending them to SEPS's Personnel Security Group for adjudication. There was no indication that OARM was using this time to resolve specific issues or obtain additional information for its internal review. Meanwhile, these attorneys worked for almost 2 years without completion of the security clearance process.⁵¹ OARM stated that it considers the end of the 18-month appointment rather than the 60-day IRTPA guideline to be its deadline for completing an attorney's security process. However, this practice causes extreme delays and results in some attorney clearances exceeding the IRTPA guideline by more than a year. We found no reason for OARM's belief that the IRTPA timeliness guidelines did not apply to its processing of attorney adjudications.

Leadership in both OARM and SEPS stated that delays in the security process for attorneys stem from OARM's limited staffing resources. OARM has only two full-time staff responsible for processing cases and sending them to SEPS for adjudication.⁵² In FY 2010, OARM received 710 completed investigations from the FBI and, in the first quarter of FY 2011, it received 300 completed background investigations. During this time, only 234 attorney security adjudications were completed. OARM stated that between September 2010 and the spring of 2011, it had an additional attorney on a detail assignment to complete adjudications. The OIG's data showed that the average timeliness for attorneys improved by 53 days during this time period. However, OARM no longer has the detail position and, due to budget restrictions, has not been able to hire additional staff.

Aside from limited resources, OARM also lacks an efficient process for managing its workload of attorney investigations and sending them to SEPS for adjudication. The OIG looked at other component processes. For example, EOUSA's process for non-attorneys hired to work in EOUSA and the U.S. Attorneys' Offices. Like attorneys, these employees receive an internal review of agency-specific requirements by EOUSA. However, instead of waiting for EOUSA to complete its review, SEPS adjudicates a case as soon as the investigation is complete. If there are any significant

⁵¹ If attorneys require access to classified information before their background investigations are completed, they may be granted interim clearances. However, the interim clearances are not based on full background investigations.

⁵² In addition to adjudicating completed background investigations, these two individuals also review pre-employment waivers for attorneys and law student interns. OARM stated that it received a total of 1,892 waiver requests between the first quarter of FY 2010 and the first quarter of FY 2011.

issues, SEPS sends the case to EOUSA security staff. However, if there are no issues, SEPS simply adjudicates the file and notifies EOUSA electronically of its decision. This reduces EOUSA's workload and ensures that it is reviewing only the most relevant cases. It also reduces the possibility that SEPS and EOUSA are duplicating processes by reviewing each file twice. At the FBI, the security clearance process for FBI attorneys is completed first by the FBI and the information is then forwarded to OARM for job-specific review. The OIG believes that OARM would benefit from a similar process like that at the EOUSA or the FBI.

Security approvals for certain key positions consistently take longer than 60 days to complete.

The OIG analyzed the time taken to complete security approvals for agents, intelligence analysts, and linguists hired between October 1, 2009, and December 31, 2010. These positions represent key functions of the Department and require access to classified information. As a result, they receive Single Scope Background Investigations and are subject to the IRTPA timeliness guidelines.

The time to complete a National Security Information clearance for agents, intelligence analysts, and linguists exceeded the 60-day guideline for all quarters analyzed.⁵³ For each of these job series, this increase was due to the time it took to complete background investigations. Additionally, adjudications for linguists were significantly longer when compared with the other positions.

Timeliness for New Agent, Intelligence Analyst, and Linguist Hires

Many positions allow employees to start under a waiver while their background investigations are being completed. However, individuals hired into agent, intelligence analyst, and linguist positions generally cannot start work until their background investigations are completed and have been favorably adjudicated. Although these positions are eventually filled with applicants whose background investigations have been favorably adjudicated, the time it takes the Department to fill them is negatively affected by the length of time it takes to complete a security clearance.

⁵³ This represents the timeliness for 100 percent of agent, intelligence analyst, and linguist cases.

Previous OIG reports also found that security clearances for intelligence analysts and linguists were taking a long time to complete, in part due to the time taken to complete the background investigations.⁵⁴

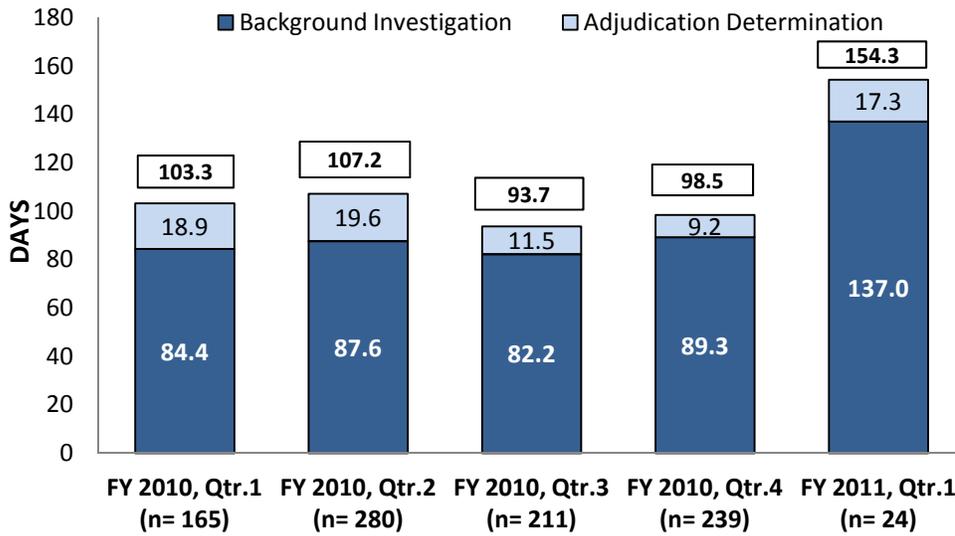
Agents

In this review, we found that the majority (79 percent) of security clearance approvals for agents exceeded the 60-day guideline in all 5 quarters, primarily due to the length of the background investigations. Ninety-one percent of background investigations exceeded the 40-day guideline. However, only 22 percent of adjudications exceeded the 20-day goal for that phase of the process. This is consistent with the OIG's determination that it was the time taken for background investigations, rather than adjudication determinations that prevented the Department as a whole from meeting the IRTPA guideline.

The average time to complete a security approval for an agent increased by nearly 60 days between the fourth quarter of FY 2010 and the first quarter of FY 2011, from 98 days to 154 days (Figure 8). All of the cases completed in the first quarter of FY 2011 exceeded 60 days, taking between 75 and 352 days to complete. In addition, 96 percent of these cases were completed by the FBI. The FBI stated that it reviews pending cases in the fourth quarter of each fiscal year and prioritizes cases that can be adjudicated quickly to meet its hiring goals, delaying cases that may take additional time to be completed until the first quarter of the following year. This may explain the longer processing times in the first quarter of FY 2011.

⁵⁴ *The Federal Bureau of Investigation's Efforts to Hire, Train and Retain Intelligence Analysts*, Audit Report 05-20 (May 2005); *Follow-up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Audit Report 07-30 (April 2007); *The Drug Enforcement Administration's Use of Intelligence Analysts*, Audit Report 08-23 (May 2008); and *The Federal Bureau of Investigation's Foreign Language Translation Program*, Audit Report 10-02 (October 2009).

Figure 8: Timeliness of Special Agent Security Approvals, October 1, 2009, through December 31, 2010



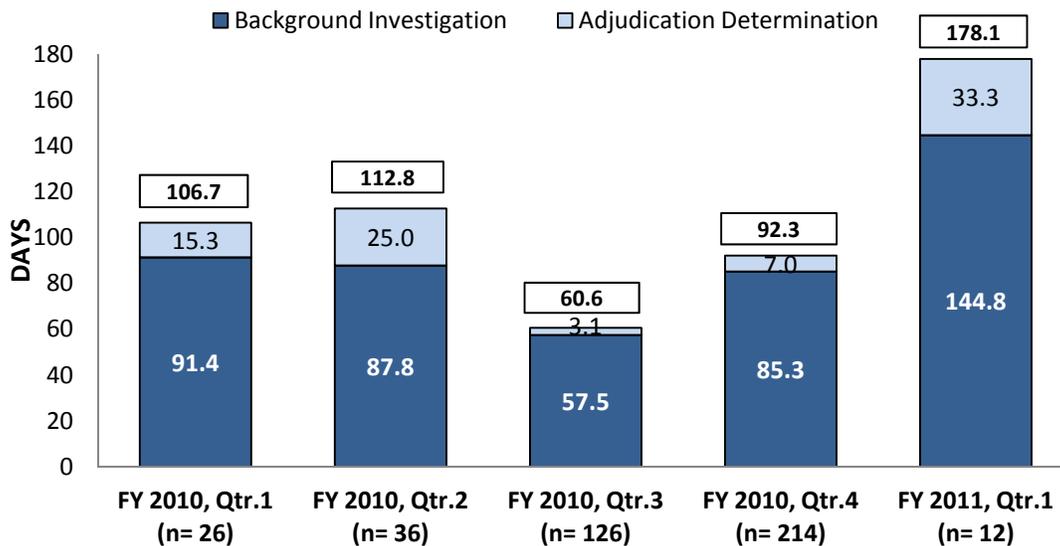
Source: OIG analysis.

Intelligence Analysts

The OIG determined that the majority (68 percent) of security approvals for intelligence analysts exceeded the 60-day guideline (Figure 9). This was due to the length of time to complete the background investigation. Eighty-three percent of background investigations exceeded the 40-day guideline. In contrast, only 10 percent of adjudications took more than 20 days to complete.

The average time to complete a security approval for an intelligence analyst increased by nearly 86 days between the fourth quarter of FY 2010 and the first quarter of FY 2011, from 92 days to 178 days. All of the cases completed in this quarter exceeded 60 days, taking between 71 and 261 days to complete. Most of the intelligence analyst cases (83 percent) completed in this quarter were conducted by the FBI. The increased times in this quarter are consistent with the FBI's explanation that it processes longer cases in the first quarter of the fiscal year.

Figure 9: Timeliness of Intelligence Analysts' Security Approvals, October 1, 2009, through December 31, 2010



Source: OIG analysis.

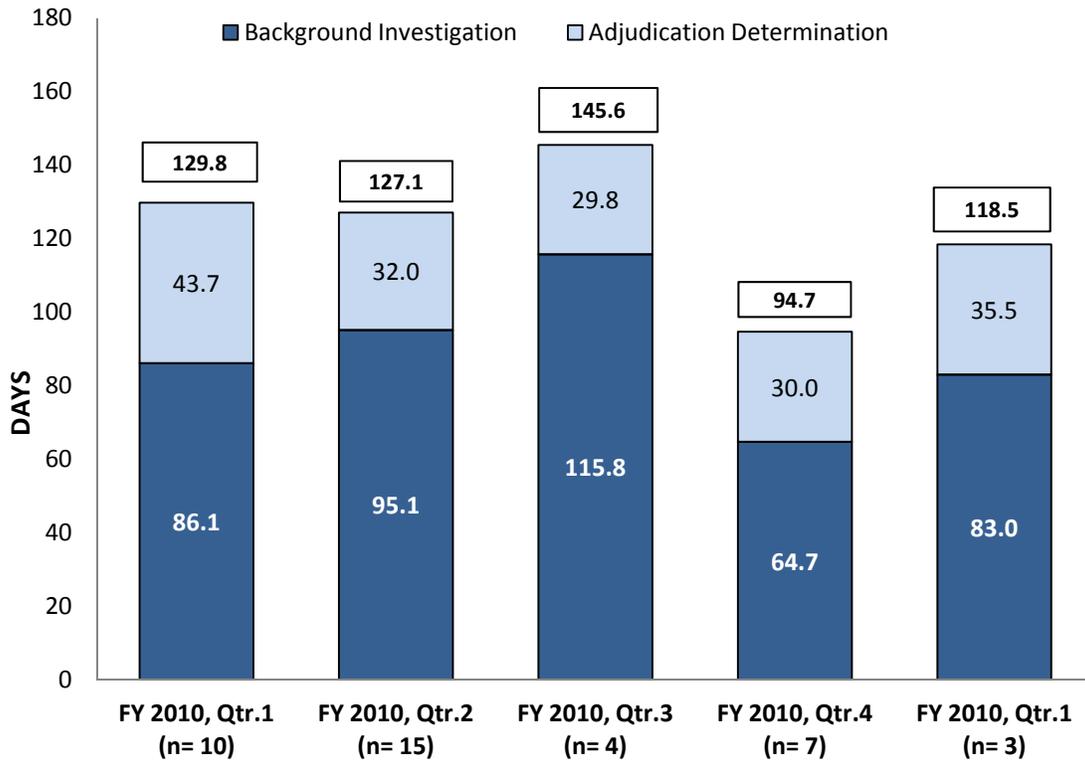
Linguists

The OIG determined that the majority (87 percent) of security approvals for linguists failed to meet the 60-day guideline (Figure 10). As with agents and intelligence analysts, background investigations for linguists exceeded the 40-day guideline, with 82 percent taking more than 40 days to complete. However, unlike adjudications for agents and intelligence analysts, 67 percent of adjudications for linguists exceeded the 20-day guideline.

Adjudications for agents and intelligence analysts generally took between 3 and 33 days to complete, while the majority of adjudications for linguists took between 30 and 44 days. The Department completed security clearances for only 39 linguists during the period of our review, and most (91 percent) were employed by the FBI.⁵⁵

⁵⁵ Most Department linguists are contractors, which may explain the relatively low number of employee hires. Contractors will be covered in the second phase of this review.

Figure 10: Timeliness of Linguists' Security Approvals, October 1, 2009, through December 31, 2010



Source: OIG analysis.

OIG Review of Agent, Intelligence Analyst, and Linguist Security Files

Human resources and security personnel, both at headquarters and in the field, stated that security clearance approvals for individuals with a large number of foreign connections or extensive overseas travel usually take longer to complete. The investigator may have to conduct additional work to contact and verify information overseas. In addition, if the individual has connections to certain countries, the hiring component may conduct a risk analysis to ensure the individual does not pose a risk to national security. Security and human resources staff stated that linguists and intelligence analysts are more likely to have these types of foreign connections, given the nature of their work. Although not unique to any specific type of position, significant credit issues are another common factor that may affect the length of time it takes to complete a security clearance. Employees must resolve any outstanding credit issues before they can be granted a clearance. This may involve showing proof of a payment plan or providing documentation demonstrating that they have paid down their debts.

The OIG examined security files for some of the longer agent, intelligence analyst, and linguist cases to determine why it took so long to process these particular individuals' security clearances. All of these cases involved significant foreign connections or credit issues that extended the security clearance process.⁵⁶ However, these cases appear to be isolated instances with extenuating circumstances and are not necessarily representative of the typical clearance process. For example, we examined two particularly lengthy cases involving agents:

- One of the longest agent cases took 352 days to process, with 337 days for the background investigation and 15 days for the adjudication. The position required a Top Secret clearance with Sensitive Compartmented Information access. The individual had a large number of foreign contacts through his spouse. During the investigation, it was discovered that the individual's spouse was not a U.S. citizen. Based on the documentation in the security file, this specific issue added at least 6 weeks to the background investigation. As a result of the lengthy investigation time, the investigator had to re-run certain checks and reports that had expired.
- Another agent case took 308 days to process, with 300 days for the investigation and 8 days for the adjudication. The position required a Top Secret clearance with Sensitive Compartmented Information access. The individual had significant credit issues that were discovered during the background investigation. This included a court-ordered lien. It took 6 months for the individual to demonstrate that the credit issue had been resolved. Meanwhile, the individual could not receive a clearance or be approved to start work. Further, as a result of the lengthy investigation time, the investigator had to re-run certain checks and reports that had expired.

Both these cases were completed during the first quarter of FY 2011 and contributed to the increase in average processing times for this period.

We also examined lengthy cases involving intelligence analysts and linguists. For example:

⁵⁶ The OIG reviewed a total of 50 cases from 9 components. Cases were selected based on the time it took to complete the investigation and adjudication for specific job series. We looked at both long and short cases. The OIG also selected cases based on the investigative agency. Only the cases relevant to initial investigations for agent, intelligence analyst, and linguist positions are discussed here.

-
-
- In one of the longest intelligence analyst cases, the background investigation took a total of 261 days to complete, and the adjudication was completed in less than a day. The position required a Top Secret clearance. The individual had significant credit issues and was required to provide extensive documentation to prove that these issues were resolved. This documentation included several years' worth of bank statements and copies of correspondence with creditors. This case was completed during the first quarter of FY 2011 and contributed to the increase in the average processing times for that period.
 - A linguist case took a total of 178 days to complete, with 125 days for the background investigation and 53 days for the adjudication. The position required a Top Secret clearance with access to Sensitive Compartmented Information. The individual was born overseas and held dual citizenship. The individual also had several foreign contacts, including family members, as well as some drug issues. The individual's security file noted that a possible foreign influence could exist, which required additional risk analysis.

Conclusions and Recommendations

The OIG concluded that the Department as a whole is not meeting the overall IRTPA time guideline of 60 days when completing security clearances for National Security Information positions, taking approximately 81 days to complete the security process. This is primarily due to the length of time taken to complete background investigations rather than adjudications. The Department failed to meet the 40-day IRTPA guideline for background investigations, averaging 66 days. However, the Department did meet the IRTPA time guideline for adjudications, averaging 15 days. The majority of cases were completed within 6 months. Further, the Department reduced its pending caseload by 79 percent during the time period covered by this review.

The Department does not include all attorneys in the data reported to OPM to measure the Department's timeliness against the IRTPA guideline. Although SEPS uploads investigation and adjudication information for attorneys into JSTARS, it does not report all of this data to OPM. Consequently, Department managers were not aware that it takes significantly longer to complete security clearance approvals for Department non-FBI attorneys than for other personnel.

Security clearance approvals for attorneys, agents, intelligence analysts, and linguists exceeded the 60-day guideline. Adjudications for agents and intelligence analysts were completed within the 20-day

guideline. However, both background investigations and adjudications failed to meet the timeliness guideline for attorney and linguist positions. Issues such as connections to foreign countries or significant credit problems seemed to cause delays in completing clearances for agents, intelligence analysts, and linguists. However, a review of the longer attorney cases showed that inefficiency in OARM's process caused delays in attorney security clearances.

To improve the Department's ability to be timely in completing the security clearance process, we recommend that:

1. OARM work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals;
2. OARM reduce the time-limited appointment waiver period from 18 months to 12 months and 1 day to complete suitability determinations;
3. OARM increase the amount of staff dedicated to processing completed investigations; and
4. SEPS work with OPM, FBI and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's IRTPA timeliness reports.

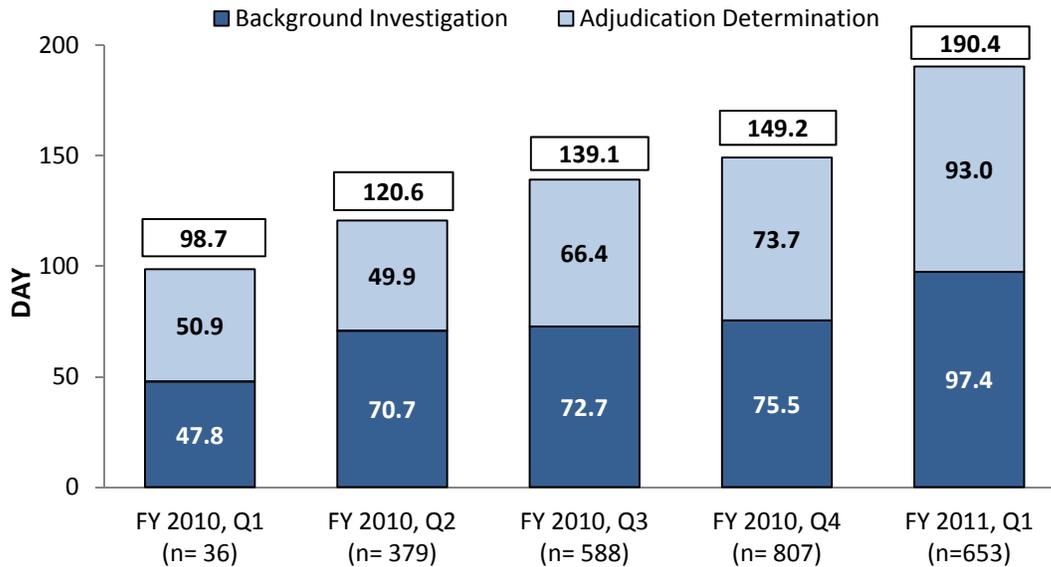
CHAPTER II: TIMELINESS FOR PUBLIC TRUST POSITIONS

The Department's time to complete Public Trust cases increased 92 percent from 99 to 190 days during the period of our review. Public Trust employees start work under a waiver while their cases are processed. As a result, these individuals routinely work in the Department, with access to sensitive information and systems, for significant periods of time without completed background investigations and adjudications.

The Department's time to complete Public Trust cases has increased, and as a result, employees routinely have access to sensitive information and systems for significant periods without a completed background investigation or adjudication.

Overall, the time to complete a Public Trust case increased by 91 days from the first quarter of FY 2010 through the first quarter of FY 2011, from 99 to 190 days (Figure 11). The time to complete background investigations for Public Trust positions increased from 48 days to 97 days. Likewise, the time to complete Public Trust adjudications increased from 51 days to 93 days. During the first quarter of FY 2011, the number of cases completed decreased by 19 percent, compared with the previous quarter. However, the Department's time to complete adjudications increased by nearly 20 days.

Figure 11: Department Timeliness in Completing Public Trust Cases, October 1, 2009, through December 31, 2010



Source: OIG analysis.

Employees in Public Trust positions generally start work under a waiver while their background investigations are being completed. Many of these individuals are in positions where they are in close proximity to sensitive systems and information. During the time period analyzed, individuals in Public Trust positions routinely worked in the Department for 3 to 6 months without a completed background investigation or adjudication. The OIG is concerned that this may present a potential security risk.

OPM conducts the background investigations for Public Trust employees, but these background investigations are not subject to any timeliness standards. OPM, however, requires agencies to report any actions they took based on an OPM investigation within 90 days of receiving a completed background investigation. The BOP, SEPS, and the USMS are the only Department components that adjudicate Public Trust cases for federal employees. The remaining components use SEPS to adjudicate their Public Trust positions. Security Managers at the BOP, SEPS, and USMS told us that they strive to meet OPM’s 90-day target for reporting their adjudication decisions. ATF, the DEA, and the FBI do not have Public Trust positions.

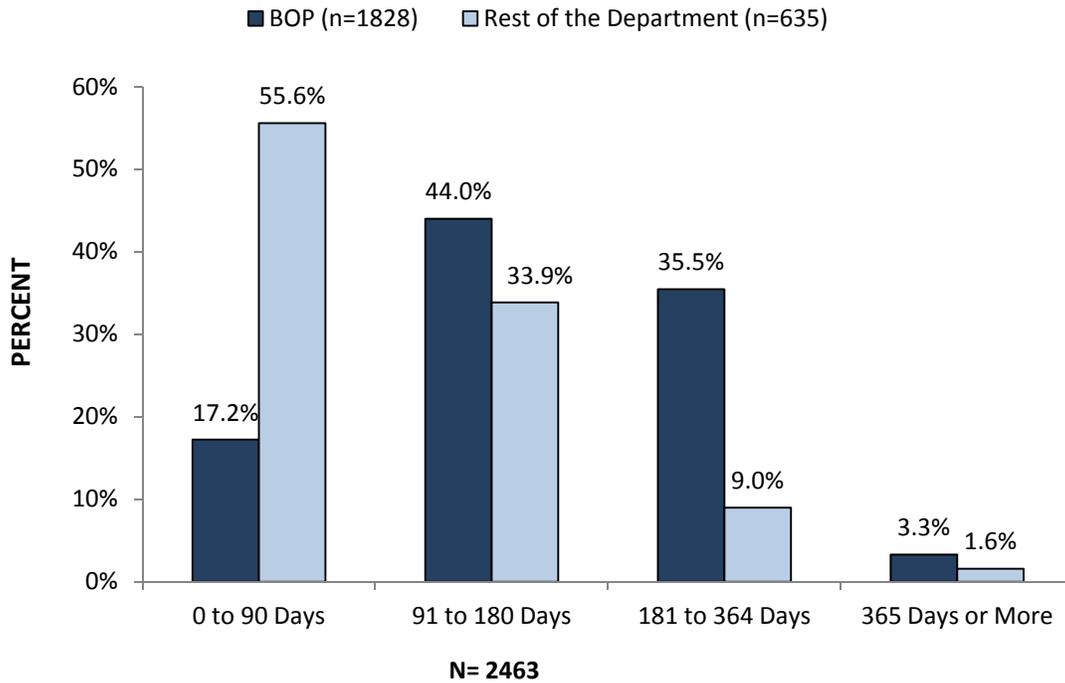
Because Public Trust employees start work under a waiver, the time it takes to complete a Public Trust case does not directly affect the Department's ability to bring individuals on board. An OPM manager stated that because investigations for security clearances have legal timeliness mandates, OPM considers those investigations to be a higher priority than background investigations for Public Trust positions.

We also found that the processing times for some Public Trust cases exceeded the 1-year probationary period. It took more than a year to complete the background investigations and adjudications for 3 percent (70 of the 2,463 positions reviewed) of the Public Trust positions. If derogatory information is not uncovered during the 1-year probationary period, employees are granted permanent status. If a background investigation then uncovers derogatory information and the Department seeks to discharge the employee, that employee has the full appeal rights of permanent employees. As a result, ensuring the completion of investigations for Public Trust positions before the end of the probationary period is important.

BOP Analysis

Because the BOP represented 74 percent of the total Public Trust cases examined during the time period of our review, we compared the time it took to complete a BOP Public Trust case with the rest of the Department's completion times (Figure 12).

Figure 12: Time to Complete BOP Public Trust Cases, October 1, 2009, through December 31, 2010



Source: OIG analysis.

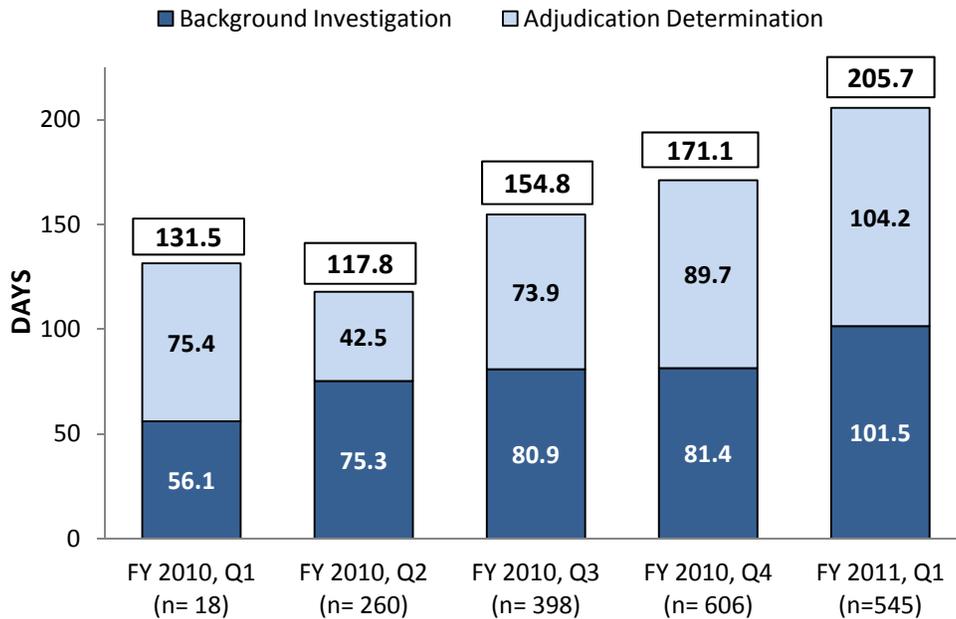
As shown above, 83 percent of BOP Public Trust cases took more than 90 days (3 months) to complete. Of those, 3 percent (60 cases) took longer than a year. In contrast, only 44 percent of the rest of the Department’s Public Trust cases exceeded 90 days, and only 2 percent (10 cases) took longer than a year. Further, only 11 percent of the Department’s cases took more than 180 days (6 months) to complete, compared with the BOP’s 39 percent.

The OIG also found that the security staff at BOP headquarters does not review an individual’s security information until the OPM investigation is completed. Given that 39 percent of BOP cases take more than 6 months to complete, these individuals are routinely working in positions with possible access to sensitive information for a considerable period of time while waiting for the security adjudication from BOP headquarters.

We further analyzed the BOP’s timeliness in completing Public Trust cases from October 1, 2009, through December 31, 2010 (Figure 13). The average number of days to complete a BOP Public Trust case increased 56 percent (from 132 days to 206 days) during that time period. The time to complete background investigations increased

82 percent, from 56 days to 102 days. Adjudications went from 75 days on average to 104 days on average, a 39-percent increase.

Figure 13: Timeliness of BOP Public Trust Cases, October 1, 2009, through December 31, 2010



Source: OIG analysis.

On average, the BOP met its 90-day goal for completing adjudications in FY 2010, averaging 70 days. However, it did not meet the goal in the first quarter of FY 2011. Even though it processed fewer cases in the first quarter of FY 2011 compared with the previous quarter, the BOP’s adjudication time increased by nearly 15 days. The trend of increasing times to complete investigations and adjudications of concern because, if they are not completed before employees finish their 1-year probation, the process for removing them if the investigations disclose disqualifying information becomes much more onerous.

Conclusions and Recommendation

On average, the Department’s Public Trust cases took more than 6 months to complete. Moreover, the average time to complete a Public Trust case increased 92 percent between the first quarter of FY 2010 and the first quarter of FY 2011. The majority of Public Trust cases were the BOP’s and took significantly longer to complete compared with the cases from rest of the Department. Only 11 percent of the Department’s cases took more than 180 days (6 months) to complete, compared with the

BOP's 39 percent. Further, because employees in Public Trust positions start work under a waiver, they have official access to sensitive information and systems without having completed background investigations.

To further improve the Department's performance in completing background investigations and adjudications for Public Trust positions, we recommend that:

5. the BOP work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases.
6. SEPS work with components to ensure that approvals for individuals in a probationary status are completed prior to the end of the probation period.

CHAPTER III: PROGRAM OVERSIGHT AND CLEARANCE TRACKING

SEPS's oversight of the Department's personnel security processes is not sufficient to identify security violations and enforce security policy. Although components track data on the status of employee background investigations, clearance levels, and reinvestigations, the tracking is inconsistent and often incomplete. Further, the field does not always have accurate information on individuals' clearance levels or the status of their investigations. The lack of information makes it difficult to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information. Further, reciprocity data is inconsistently tracked, not reported, or reported incompletely, which made it impossible to determine whether the Department applies reciprocity consistently.

SEPS's oversight is not effective in identifying security violations and enforcing security policy across the Department.

SEPS provides Department-wide oversight of the security clearance program, primarily through its Compliance Review Team. The team conducts site visits of both headquarters and field offices to determine if components are complying with the Department's policies for personnel (including contractors), document, physical, information technology, and communications security, continuity of operations, and for occupant emergency plans, along with the Department's safety and health program. Through these reviews, the Compliance Review Team identifies security violations and provides the components with corrective actions and recommendations for improving their security processes. The team shares any issues related to both National Security Information and Public Trust positions with the SEPS Personnel Security Group.

The Compliance Review Team completed 54 reviews covering 55 offices in FY 2010 and in the first quarter of FY 2011 (see Appendix VIII). This is a relatively small number considering that the Department has over 3,500 offices world-wide. The Compliance Review Team's abilities are limited, in part, by having only three full-time staff to conduct site visits. In addition, the team canceled 27 planned site visits for FY 2011 because of budget cuts.

The Compliance Review Team's limited capabilities directly affect SEPS's ability to enforce DOJ's security policies. For example, when we reviewed the BOP's delegation of authority memorandum, we noted that SEPS had given the BOP Security Programs Manager authority to sign pre-employment waivers in 2003. The memorandum stated that the Security Programs Manager cannot further delegate any of the responsibilities. However, when the OIG visited four BOP facilities, we found that the wardens were approving the pre-employment waivers for employees, with the Security Programs Manager's knowledge, in violation of the BOP's delegated authority.

The Compliance Review Team conducted 11 reviews of BOP facilities between 2005 and 2010 but did not uncover this issue because the team did not look at the BOP personnel security files. A file review is normally a part of the Compliance Review Team's procedures. However, the BOP's Security and Background Investigation Section (SBIS) maintains the personnel security files from all BOP facilities at a central location. As a result, the team could not examine files for the facilities it reviewed during its site visits, and the team did not request files from the SBIS for those facilities.⁵⁷

In another case, in response to an OIG data request in February 2011, ATF discovered that 24 employees had entered on duty and worked for almost a year without holding the required security clearance. The Compliance Review Team had visited ATF headquarters in November 2010, but did not find this or any other unresolved personnel security issues.⁵⁸

Most offices the OIG visited did not mention the Compliance Review Team when asked about the Department's oversight activities. Three security unit chiefs told the OIG they had never even heard of the Compliance Review Team. Security personnel at ATF, DEA, and FBI field offices and BOP facilities stated that they are subject to periodic reviews from their own headquarters that include a review of their personnel security practices. However, these components do not coordinate their oversight activities with either the Compliance Review Team or the Personnel Security Group, nor do they share the results of their internal

⁵⁷ SEPS eventually discovered the issue in January 2011. However, it was only after an SBIS employee raised it during a training session rather than as part of oversight review procedures or any proactive efforts. As of late August 2011, SEPS and the BOP were working together to resolve the issue.

⁵⁸ ATF personnel told the OIG that the human resources staff had failed to notify the Personnel Security Branch that the 24 individuals had entered on duty.

reviews with SEPS. The Personnel Security Group Assistant Director confirmed that SEPS was not aware that the components even had their own internal review processes. Not sharing results limits SEPS's ability to identify Department-wide security issues and trends, effectively leverage the Compliance Review Team's limited resources, and reduce the possibility for duplication between the Compliance Review Team's oversight and components' internal reviews. If such information were shared, SEPS may attain greater efficiencies and could oversee security reviews on a broader range of components. In addition, this coordination could result in potential savings because SEPS may not need to conduct as many reviews.

Personnel security data is not consistently tracked and managed across the Department nor made available to the field so that security staff can ensure that only individuals with the appropriate clearance level have access to sensitive and classified information.

Procedures for tracking personnel security data, including data on clearance levels and reinvestigations, vary significantly throughout the Department. The FBI uses its Automated Case System to track background investigations on government employees and to run reports on those investigations. Similarly, it uses its Facility Security System to both track background investigations and run reports on those investigations on contractors and on law enforcement officers from other agencies who are to serve on FBI task forces. Both systems allow authorized FBI staff in the field to look up individuals' clearance levels by case number and show the status of ongoing cases. Although the BOP, DEA, and USMS have their own systems for tracking security information, they do not provide detailed information to personnel in the field. ATF headquarters officials stated that they send quarterly reports to field office management. However, the OIG found that Division Operations Officers, who are responsible for overseeing the personnel security process in the field, did not always receive the information.

With the exception of the FBI, most personnel security information is centralized at component headquarters, and personnel in the field offices have little to no access to the security data for their employees. As a result, many of the security personnel in the field offices maintain their own paper files, spreadsheets, rosters, or databases to aid them in managing the security information for their employees. To check on the status of an individual's clearance, they usually have to contact headquarters. This can result in the components' field operations having conflicting or incomplete information for the individuals they employ. We found six instances at three different components, described below, in which security personnel were unaware of overdue reinvestigations or of

the clearance levels held by their employees. These problems might have been avoided if the field had access to its headquarters security information or better tracking mechanisms.

- At two separate ATF field offices, the Division Operations Officers responsible for overseeing the personnel security process there stated that they believed that all ATF employees had Top Secret clearances and therefore, they did not need to regularly check or verify the security clearances for employees working in their divisions. However, while preparing for the OIG's visit, one of those Division Operations Officers reviewed a roster and discovered that at least four individuals whom she believed had Top Secret clearances were only cleared to the Secret level. Further, an OIG review of ATF data also showed that 25 of the 147 (17 percent) ATF employees who had a security clearance completed between October 1, 2009, and December 31, 2010, received less than a Top Secret clearance. Although we did not find any instances where individuals accessed information without the proper clearance level, the automatic assumption that all individuals have the same clearance level poses a potential security risk.
- At the BOP, the SBIS notifies human resources managers in the field when employees are coming up for reinvestigation. However, the human resources personnel at one BOP facility stated that a recent reinvestigations list included one individual who had been overdue since 2007 and several employees who no longer worked at the facility. These individuals had not appeared on previous reinvestigations lists even though they had been overdue for some time.
- At a USMS field office we were told that a management analyst had had a reinvestigation due in 2003. The analyst submitted the forms to OPM, but was notified that the forms had passed through a post office that was infected with anthrax and were never delivered to OPM. The analyst tried unsuccessfully to resubmit the forms using e-QIP and eventually sent them through certified mail. However, as of June 2011 the analyst still had not received confirmation that the reinvestigation was complete. The OIG checked OPM's Central Verification System and verified the individual's most recent reinvestigation was conducted in 2003. However, the analyst was due for another reinvestigation in 2008 that was never initiated. As of July 17, 2011, the analyst was working without an active clearance.

Consistent tracking procedures and field access to data would detect these types of cases. We believe implementing JSTARS will ensure that security data is tracked consistently across the Department and will give SEPS greater oversight over components' timeliness. ATF, the BOP, DEA, and USMS were scheduled to begin tracking their information in JSTARS by the end of 2011. Although the FBI will continue to maintain its own separate system because it has classified data, it planned to start regularly uploading unclassified data to JSTARS in early 2012.

While JSTARS should improve the Department's oversight at the headquarters level, most field offices will still be unable to view security data. Currently, only one component plans to use JSTARS capabilities to improve information sharing with the field. EOUSA is granting limited JSTARS access to District Security Officers in the U.S. Attorneys' Offices nationwide. SEPS specifically recommended that the BOP consider granting JSTARS access at its facilities. Although, the BOP would benefit from some of the automation features in JSTARS, it has not made any plans to implement this recommendation. Because the BOP currently relies on a paper process to notify facilities when a background investigation has been adjudicated, the OIG agrees with SEPS that BOP personnel in the field would benefit from being able to view active cases in JSTARS.

Reciprocity is not consistently tracked or properly applied, which can cause delays and increase costs for the Department.

The reciprocity provision in IRTPA mandates that agencies accept a background investigation completed by any other authorized federal investigative or adjudicative agency provided that the clearance is not temporary or interim, and the background investigation was favorably adjudicated, was at the right security clearance level for the position, and was completed within the past 5 years.⁵⁹

Reciprocity data is not tracked consistently across the Department. As a result, we could not determine if components are meeting the reciprocity requirement outlined in IRTPA and Executive Order 13467. There is currently no requirement to track reciprocity, which makes it difficult to determine if efforts are duplicated during the personnel security process.

The OIG requested reciprocity data from ATF, the BOP, DEA, FBI, SEPS, and USMS. The DEA, SEPS, and USMS provided some reciprocity

⁵⁹ Executive Order 12968 and Executive Order 13381 also include the requirement for reciprocity.

data. However, the data we did receive did not always contain the type of background investigation used as the basis for reciprocity. It also was missing other information, such as the date the individual's background investigation was requested, received, or adjudicated. ATF, the BOP, and the FBI could not provide any reciprocity data.

Because of the lack of reciprocity tracking data, the OIG reviewed 50 personnel security files to determine if any of these cases were eligible for reciprocity.⁶⁰ Of those 50 cases, we found 11 cases where the individual had a background investigation that met the requirements of the position and was less than 5 years old. Reciprocity was properly applied for 10 of these 11 cases. In the one case where reciprocity was not applied, the component agreed that it erroneously completed a new investigation.

Further, we found indications that reciprocity is not always applied in the field at BOP facilities. In interviews, BOP personnel at four facilities we visited repeatedly told the OIG that they will initiate a new background investigation, even if an applicant already has a valid background investigation. This is a duplication of effort that results in unnecessary costs and is not consistent with the reciprocity guidelines. Based on the costs of an initial investigation, failing to apply reciprocity can result in additional costs ranging from \$752 to \$4,005, depending on the investigative agency and the type of investigation.⁶¹ If the Department required components to track reciprocity, it would be able to mitigate unnecessary spending and ensure that components apply reciprocity when appropriate.

Conclusions and Recommendations

Part of SEPS's responsibility is to use the Compliance Review Team to provide oversight of the Department's personnel security process. Although the Compliance Review Team conducts site visits to determine the Department's compliance with security programs, its ability to conduct routine and follow-up site visits is limited by its resources and the broad scope of its responsibilities. During FY 2010 and the first quarter of FY 2011, the team completed 54 reviews at 55 of the Department's 3,500 offices. As a result, the Compliance Review Team is not effective in detecting systemic security process violations or

⁶⁰ The files were selected across all components. Appendix V details the methodology used to select and review files.

⁶¹ See Appendices II and V for a list of costs by investigative agency and the methodology used to determine background investigation costs for this report.

Department-wide trends. In addition, there is no requirement for components to share the results of their internal reviews with SEPS to assist with identifying security issues Department-wide.

Methods to track the status of investigations and manage who had what type of clearance vary by components. We found that not all field offices have access to their component's central database of security clearance information. Those without direct access must request information from their headquarters, which means clearance information, is not always readily available. As a result, components do not always know the status of ongoing clearances, when reinvestigations are due, or who has which type of clearance. Although some offices maintain rosters of clearance information, they do not always verify employee clearances and access levels. As a result, individuals without the proper clearance level could gain access to sensitive or classified information.

The Department requires security clearance reinvestigations every 5 years. Yet, neither the Department nor component headquarters security procedures require tracking due dates for reinvestigations or procedures for coordinating with individuals to ensure reinvestigations are completed. Individuals in the field believed that reinvestigations were tracked at the headquarters level and that headquarters coordinates directly with the individual to ensure reinvestigations are completed when due. However, this does not always happen, and the OIG found instances where employees with access to sensitive and classified information had reinvestigations that were past due.

There is no Department-wide requirement or procedure to track or measure whether reciprocity is applied. Although, some components track reciprocity, the information is often incomplete. The lack of tracking mechanisms prevents the OIG from identifying unnecessary investigations; however, we found examples of components not applying reciprocity. For example, officials from the BOP stated that they always initiate a new investigation, even if an applicant already has a valid background investigation. If the Department required components to track reciprocity, it would be able to mitigate unnecessary spending and ensure that components apply reciprocity when appropriate.

To ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that:

7. the Department require components to share internal review results with SEPS,

-
-
8. the Compliance Review Team use the results of components' internal reviews to identify trends and recurring personnel security problems across the Department and focus on the most critical security issues,
 9. SEPS increase the amount of staff dedicated to conducting compliance reviews,
 10. SEPS ensure that only the BOP Security Programs Manager authorize pre-employment waivers, based on the SEPS delegation of authority memorandum,
 11. the components develop and implement procedures to ensure field offices have access to headquarters' security information,
 12. the components require each field office to know the type of clearance each employee holds on site, and
 13. the Department require components to track and report reciprocity data.

CONCLUSION AND RECOMMENDATIONS

The Department as a whole is not meeting the overall IRTPA time guideline of 60 days when completing National Security Information clearances for new federal employees. In fact, the Department exceeded the IRTPA time guideline by 21 days for the time period covered in this review.

Security clearance approvals for certain key positions take longer to complete than others. Our data analysis for agents, intelligence analysts, and linguists identified specific factors, such as foreign connections and credit issues, which contribute to the length of the security clearance process for the individuals hired into these positions. Non-FBI attorney clearance approvals take more than twice as long to complete than clearances for other federal employee positions. OARM's current entering on duty policy for new attorneys contributes heavily to the length of the security clearance process. Furthermore, because the Department does not report timeliness data on all attorneys, Department managers were not aware that it takes significantly longer to complete clearance approvals for non-FBI attorneys than for other personnel.

Completing Public Trust cases more quickly is not a priority. In fact, the average time to complete a Public Trust case increased 92 percent between the first quarter of FY 2010 and the first quarter of FY 2011. Roughly 3 percent of the Department's Public Trust cases took more than a year to complete. During this time, employees in Public Trust positions were able to work in the Department, with official access to sensitive information and systems, but without completed background investigations. We also found that the majority of Public Trust cases were for BOP employees. The BOP took significantly longer than the rest of the Department to complete Public Trust cases. Only 11 percent of the Department's Public Trust cases took more than 180 days to complete compared with 39 percent of the BOP's cases.

The Department provides limited oversight of components' security clearance processes, in part due to the size of SEPS's staff and the broad scope of its responsibilities. As a result, it is difficult to identify the critical security problems across the Department, determine if components comply with the Department's security programs, and enforce the Department's security policies.

Finally, we found that the Department is not tracking the components' compliance with IRTPA's reciprocity mandate and that at least one component was not in compliance with reciprocity

requirements. This can result in delays and unnecessary costs of between \$752 and \$4,005, depending on the investigation type.

To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that:

1. OARM work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals;
2. OARM reduce the time-limited appointment waiver period from 18 months to 12 months and 1 day to complete suitability determinations;
3. OARM increase the amount of staff dedicated to processing completed investigations;
4. SEPS work with OPM, FBI and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's IRTPA timeliness reports;
5. the BOP work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases;
6. SEPS work with components to ensure that approvals for individuals in a probationary status are completed prior to the end of the probation period.
7. the Department require components to share internal review results with SEPS;
8. the Compliance Review Team use the results of components' internal reviews to identify trends and recurring personnel security problems across the Department and focus on the most critical security issues;
9. SEPS increase the amount of staff dedicated to conducting compliance reviews;
10. SEPS ensure that only the BOP Security Programs Manager authorize pre-employment waivers as prescribed in the SEPS delegation of authority memorandum;

-
-
11. the components develop and implement procedures to ensure field offices have access to headquarters' security information;
 12. the components require each field office to know the type of clearance each employee holds on site; and
 13. the Department require components to track and report reciprocity data.

APPENDIX I: ACRONYMS

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BI	Background investigation
BICS	Background Investigation Contract Service
BOP	Federal Bureau of Prisons
DEA	Drug Enforcement Administration
DOJ	Department of Justice
e-QIP	Electronic Questionnaires for Investigations Processing
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FIS	Federal Investigative Services
FY	Fiscal year
HSPD-12	Homeland Security Presidential Directive 12
IRTPA	<i>Intelligence Reform and Terrorism Prevention Act of 2004</i>
JMD	Justice Management Division
JSTARS	Justice Security Tracking and Adjudication Record System
MBI	Moderate Background Investigation
NACI	National Agency Check and Inquiries
OARM	Office of Attorney Recruitment and Management
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SBIS	Security and Background Investigation Section
SCI	Sensitive Compartmented Information
SEPS	Security and Emergency Planning Staff
SIGBIU	Special Inquiries and General Background Investigations Unit
SSBI	Single Scope Background Investigation
USAO	United States Attorney's Office
USMS	United States Marshals Service

**APPENDIX II: RISK LEVELS AND COST ASSOCIATED WITH
BACKGROUND INVESTIGATION REQUIREMENTS FOR NATIONAL
SECURITY INFORMATION AND PUBLIC TRUST POSITIONS**

Section 731 of Title 5, C.F.R. requires that each Department position be designated with a risk level depending on the position’s potential to adversely affect the integrity and efficiency of the agency’s service. Positions are designated as Public Trust unless access to National Security Information is required. If the position requires access to National Security Information, it is assigned a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Non-Critical Sensitive. Positions with a Special-Sensitive designation require access to Sensitive Compartmented Information (SCI) and are assigned to individuals with Top Secret clearances. Table 6 summarizes the various risk and sensitivity levels and the background investigation required for each position.

Table 6: Risk and Sensitivity Levels and Their Required Background Investigations

Position Sensitivity Level	Risk Level	Access level				Initial Background Investigation Required
		Confidential	Secret	Top Secret	SCI	
National Security Information Positions						
Special Sensitive	4				X	SSBI
Critical Sensitive	3			X		SSBI
Non-Critical Sensitive	2	X	X			MBI or BI (5-year scope)
Public Trust Positions						
High Risk	6	NO ACCESS				BI (5-year scope)
Moderate Risk	5					MBI
Low Risk	1					NACI

A single scope background investigation (SSBI) covers the past 7 years of a subject’s activities (or to age 18, whichever is less). It includes verification of citizenship and date and place of birth, as well as national agency records checks on the subject’s spouse or cohabitant, interviews with selected references, and former spouses.

A 5-year scope background investigation (BI) is similar to a SSBI, except it only covers the past 5 years of a subject’s activities.

A moderate background investigation (MBI) consists of a personal subject interview and written inquiries covering a subject’s employment, education, credit, and residence.

A national agency check and inquiries (NACI) investigation consists of searches covering an individual’s background during the past 5 years. It does not include a personal subject interview.

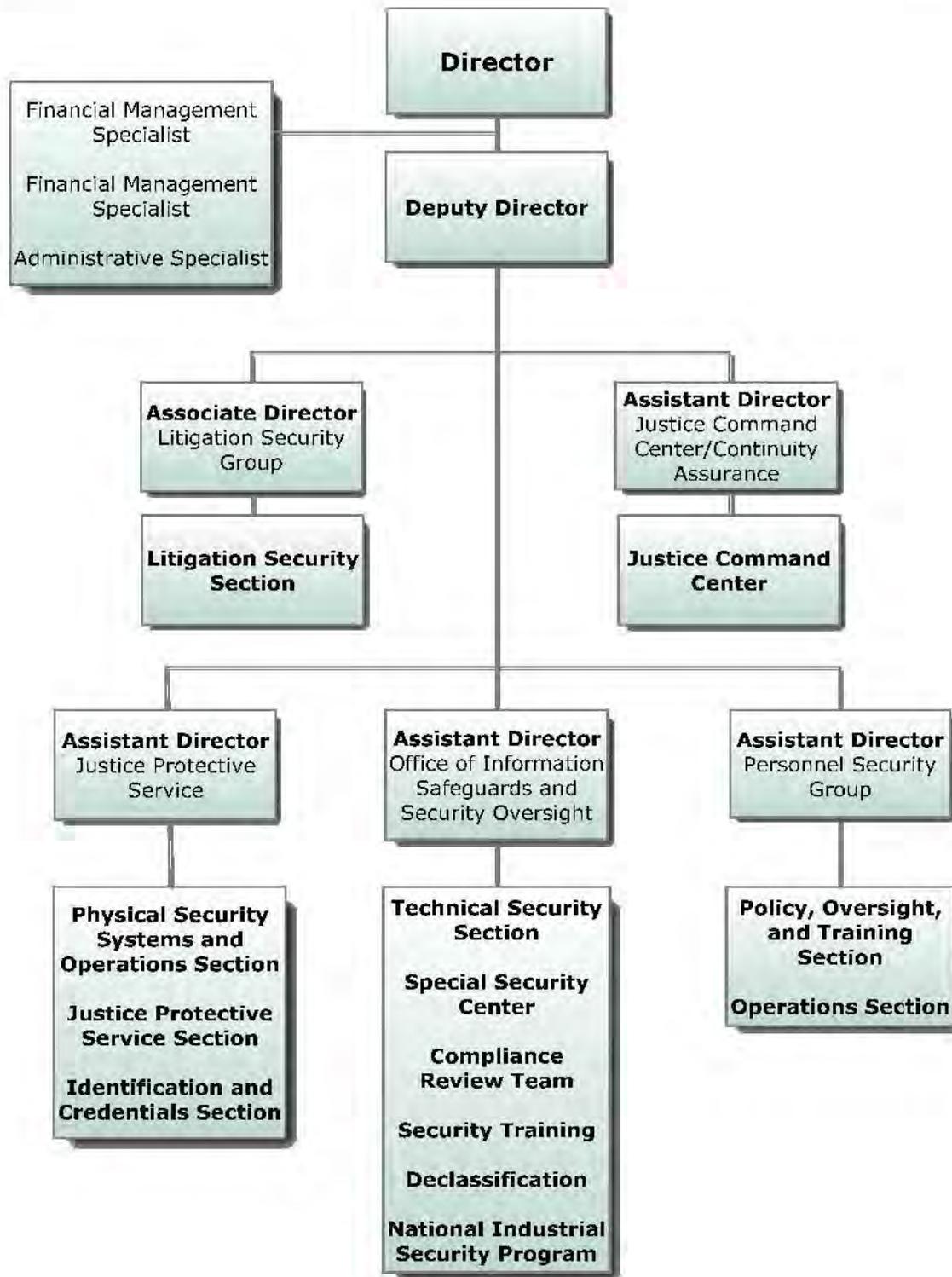
The OIG requested documentation from each of the three investigative authorities (OPM, the FBI, and ATF) regarding the direct costs of a completed background investigation. Because cost information was not available from each investigative authority for each type of investigation, Table 7 reflects only the costs associated with a moderate background investigation and a single scope background investigation when conducted by the OPM, FBI or ATF.

Table 7: Costs to Complete Background Investigations

Investigative Agency	SSBI	MBI
OPM	\$4,005	\$752
FBI	\$3,857	*
ATF	\$2,200	*

* The FBI does not conduct any MBIs. ATF has some employees that require an MBI but ATF uses OPM to conduct those investigations.

APPENDIX III: SEPS ORGANIZATION CHART



APPENDIX IV: INTERVIEWS

Component	Position
ATF	Chief of Security and Emergency Programs
	Chief Personnel Security Branch
	Contractor Team Leader
	Division Operations Officer
BOP	Chief, Security Programs Manager Unit
	Senior Secure Institution Manager
	Contracting Officer Technical Representative
	Contract Specialist
	Human Resources Bureau Manager
	Human Resources Specialist
	Assistant Administrator, Correctional Programs Specialist (Privatization Management Branch)
	Security Specialist
Consolidated Executive Office	Security Programs Manager
	Director/Assistant Director of Human Resources
	Assistant Director of Procurement
Civil Division	Security Programs Manager
	Property and Facilities Management Chief
	Personnel Chief
	Acting Director for the Office of Litigation
Civil Rights Division	Security Programs Manager
	Security Specialist (Alternate Security Programs Manager)
	Human Resources Specialist
Criminal Division	Director/Security Programs Manager of Security and Operations Staff
	Physical Security Specialist/Alternate Security Programs Manager
DEA	Assistant Deputy Chief Inspector (Headquarters)

Component	Position
	Division Security Officers
	Assistant Administrative Officer
	Division Contracting Officer Technical Representative
	Personnel Liaison Specialist
EOUSA	Chief, Personnel Security Sections
	Personnel Security Specialist
FBI	Unit Chiefs in FBI Security Division
	Associate Chief Security Officer
	Human Resources Program Manager
	Assistant Section Chief
	Human Resources Assistant
	Contracting Officer Technical Representative
	Personnel Security Specialist
	Administrative Specialist
Government Accountability Office	Team Leader, Director
OARM	Director
OARM	Deputy Director
OIG	Personal Security Specialist
OPM	Program Managers
SEPS	Assistant Director, Personnel Security
	Assistant Director, Office of Information Safeguards and Security Oversight
	Chief, Compliance Review Team
	Security Specialist, Compliance Review Team
USAOs	Director of Administration
	Regional Security Specialist
	Human Resources Manager
	Human Resources Officer

Component	Position
	Human Resources Assistant
	Management Specialist
USMS	USMS, Chief Office of Security Programs
	Administrative Support Specialist
	Management and Program Analyst
	Judicial Security Inspectors
	Contracting Officer Technical Representatives

APPENDIX V: METHODOLOGY

This review employed a multi-disciplined approach consisting of evaluation of security policies and procedures, data analysis, case files review and site visits. We conducted site visits to 14 ATF and FBI field offices, USMS and USAO district offices, DEA division offices, and BOP confinement facilities in Los Angeles and Atlanta. We also visited JMD and each law enforcement component's headquarters, as well as the Civil Division, the Civil Rights Division, the Criminal Division, EOUSA, and OARM.

Six types of analyses were conducted. The methodology of each analysis is described below.

National Security Information Timeliness Using the IRTPA Guidelines

Our analysis measured the average time to complete a security clearance for the fastest 90 percent of cases completed between October 1, 2009, and December 31, 2010, by quarter. We used the "adjudication complete" date to determine which cases were completed in each quarter. The data available for analysis contained 5,204 cases.

We conducted a separate analysis to identify the fastest 90 percent of cases, within each quarter. A total of 4,684 cases were identified among the three investigative agencies – ATF (138 cases), the FBI (3,043 cases), and OPM (1,503 cases). These cases were used to calculate the average time taken to complete background investigations and adjudication determinations for National Security Information clearances for the entire Department. This analysis also included a distribution analysis through which the percentage of the Department's National Security Information cases exceeding the 60-day IRTPA guideline was determined.

We also analyzed the slowest 10 percent of all newly hired employees' cases to identify any factors that contributed to additional processing time.

Attorneys (except for FBI attorneys) were excluded from this analysis because the Department does not report attorney information to OPM to be included in its timeliness calculations. FBI attorneys (n=28) were included because the FBI includes attorneys in its IRTPA timeliness reports. A separate analysis of component attorneys was conducted.

Analysis of the Time to Complete National Security Information Cases

The OIG analyzed cases that did not have either an “adjudication completed” date or a “background investigation completed” date. Cases that did not have an “investigation initiated” date were excluded from our analysis because we could not determine when the security process started for those cases. Lastly, we analyzed cases that contained both a “background investigation completed” date and an “adjudication completed” date. We discuss each in the following paragraphs.

No “Adjudication Completed” Date or “Background Investigation Completed” Date: These cases represent those that are pending an investigation completion date and have not been adjudicated. These cases are considered to be active. Cases were assigned an “adjudication completed” date of April 25, 2011, to calculate how many days the cases had been pending. The cutoff date was chosen because that was the deadline the OIG gave components to submit their data.

Using these criteria, we identified four cases that we considered still pending either a background investigation or adjudication determination as of April 25, 2011.

No “Adjudication Completed” Date: These cases represent those that have a completed investigation but are pending adjudication. These cases are considered to be active. Cases were assigned an “adjudication completed” date of April 25, 2011, to determine how many days the case had been pending. April 25, 2011, was chosen because that is the deadline the OIG gave components to submit their data. Cases that were less than 61 days old were excluded as were Public Trust cases. Using these criteria, we identified 230 cases that were still pending an adjudication determination as of April 25, 2011.

Cases Containing both a “Background Investigation Completed” Date and an “Adjudication Completed” Date: These cases represent those that have completed all phases of the security clearance process and are not pending in status. This analysis differs from the previous analysis in that these cases were not assigned the generic “adjudication completed” date of April 25, 2011, since each adjudication date is exclusive to an individual case. We calculated the difference between the “adjudication completed” date and the “investigation initiated” date to determine the total number of days taken to complete the security clearance process. Using these criteria, we identified that 3,589 of the Department’s 5,204 (69 percent) National Security Information cases processed from

October 1, 2009, through December 31, 2010, failed to meet the overall IRTPA time standard.

Measuring Timeliness for Public Trust Positions

Our analysis measured the average time to complete a background investigation and adjudication for Public Trust cases completed between October 1, 2009, and December 31, 2010, by quarter. We used the “adjudication complete” date to determine which cases were completed in each quarter. The data available for analysis contained 2,463 cases. The average was taken using 100 percent of cases because the IRTPA timeliness guidelines do not apply to Public Trust positions. Attorneys were excluded from this analysis because background investigations and adjudication determinations for attorneys are subject to the IRTPA timeliness guidelines.

Job Series Analysis

We conducted a separate analysis to calculate the average time to complete a security clearance approval for agents, intelligence analysts, linguists, and attorneys. We reviewed the data submitted by ATF, the FBI, and SEPS for security clearances completed between October 1, 2009, and December 30, 2010, and identified 919 agent cases, 414 intelligence analyst cases, 39 linguist cases, and 234 attorney cases. FBI attorney cases were excluded from the attorney analysis because these cases are contained within the National Security Information timeliness analysis using the IRTPA guideline.

The average time to complete a security clearance approval was calculated for each of the selected job series within each quarter. The average was calculated using 100 percent of all cases.

Reciprocity Files Review

We judgmentally selected and reviewed 50 files to determine whether the Department applies reciprocity according to IRTPA mandates and Executive Orders. We selected files from each of the three investigative agencies – the FBI, ATF, and OPM. We selected files for agents, intelligence analysts, linguists, and attorneys for review because their clearances typically took longer to complete than those for other employees. In addition, we reviewed the two cases that were the longest and shortest to complete for agents, intelligence analysts, linguists, and attorneys. We also selected BOP files for review to ensure the analysis included Public Trust files.

Background Investigation Costs

The OIG reviewed FBI, ATF, and OPM background investigation cost data to identify potential cost savings associated with applying reciprocity. The investigative agencies submitted data that included fixed, variable, and indirect costs, but for this report we used only direct cost data. Direct cost data included costs for activities such as conducting interviews, compiling interview reports, and travel to and from interviews. It does not include costs for things such as overhead support staff, office space, and information system upgrades.

**APPENDIX VI: TIME TO COMPLETE NATIONAL SECURITY
INFORMATION CASES PROCESSED AS PART OF THE FASTEST
90 PERCENT**

To determine what percentage of the Department’s caseload for the fastest 90 percent of completed clearances consisted of cases that were more than 60 days old, the OIG identified cases that took more than 60 days to complete, by quarter, between October 1, 2009, and December 31, 2010. Table 8 below shows the number of cases, by quarter, which took 61 days or more to complete all phases of the security process.

Table 8: Completed Cases Processed, by Quarter

FY 2010, Quarter 1

Investigative Agency	Number of Completed National Security Information Cases Processed			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	79	190	10	3
FBI	124	334	46	1
ATF	8	14	0	0
DOJ (n=809)	211	538	56	4

FY 2010, Quarter 2

Investigative Agency	Number of Completed National Security Information Cases Processed			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	63	334	35	2
FBI	126	382	62	2
ATF	18	14	3	0
DOJ (n=1041)	207	730	100	4

FY 2010, Quarter 3

Investigative Agency	Number of Completed National Security Information Cases Processed			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	83	278	53	1
FBI	373	390	24	2
ATF	55	3	0	0
DOJ (n=1262)	511	671	77	3

FY 2010, Quarter 4

Investigative Agency	Number of Completed National Security Information Cases Processed			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	96	234	56	9
FBI	530	748	36	2
ATF	5	14	2	0
DOJ (n=1732)	631	996	94	11

FY 2011, Quarter 1

Investigative Agency	Number of Completed National Security Information Cases Processed			
	0-60 days	61-180 days	181-365 days	366 days or more
OPM	53	139	16	6
FBI	2	94	38	1
ATF	0	5	6	0
DOJ (n=360)	55	238	60	7

Table 9: Percentage of Fastest 90 Percent National Security Information Cases that Were More than 60 Days Old, by Quarter

Quarters	Investigative Agency							
	DOJ		OPM		FBI		ATF	
	More than 60 Days	Total	More than 60 Days	Total	More than 60 Days	Total	More than 60 Days	Total
FY 2010, Qtr.1	517 (71%)	728	183 (69.9%)	262	320 (72.1%)	444	14 (63.6%)	22
FY 2010, Qtr.2	730 (78%)	937	334 (84.1%)	397	382 (75.2%)	508	14 (43.8%)	32
FY 2010, Qtr.3	625 (55%)	1,136	255 (75.4%)	338	367 (50%)	740	3 (5.2%)	58
FY 2010, Qtr.4	928 (60%)	1,559	213 (69%)	309	703 (57%)	1,233	12 (71%)	17
FY 2011, Qtr.1	269 (83%)	324	144 (73.1%)	197	116 (98.3%)	118	9 (100%)	9
Overall Totals	3,069 (65.5%)	4,684	1,129 (75.1%)	1,503	1,888 (62%)	3,043	52 (37.7%)	138

Note: Percentages in “More than 60 Days” columns indicate the percentage of National Security Information cases that took more than 60 days to complete.

**APPENDIX VII: CASES PENDING AS OF
APRIL 25, 2011**

The OIG identified cases that were still pending as of April 25, 2011. Table 10 shows the number of days each case was pending, by investigative agency.

Table 10: Pending Cases, by Investigative Agency

OPM

Status of Case	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
Pending Investigation	3	4	4	12
Pending Adjudication	6	21	51	63
Total (n=164)	9	25	55	75

FBI*

Status of Case	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
Pending Investigation	0	15	18	0
Pending Adjudication	0	11	10	11
Total (n=65)	0	26	28	11

ATF

Status of Case	Days in Process			
	0-60 days	61-180 days	181-365 days	366 days or more
Pending Investigation	0	0	0	0
Pending Adjudication	0	0	0	1
Total (n=1)	0	0	0	1

* The OIG requested cases that were initiated prior to December 31, 2010, and were still pending as of April 25, 2011. The FBI was able to provide data only on cases that were initiated between May 1, 2010, and December 31, 2010. The FBI stated that data for cases initiated prior to May 1, 2010, was unreliable and it was not able to validate it. The OIG did discover 11 FBI cases in the SEPS security data that had been pending for 366 days or more. The OIG also discovered two additional cases that were pending between 181 and 365 days but were not included in the FBI's submission of pending cases. These cases were included in the SEPS data because they were FBI attorneys. The OIG included these 13 cases in the table above.

**APPENDIX VIII: COMPLIANCE REVIEW TEAM SITE VISITS,
FY 2010 AND FY 2011**

The Compliance Review Team conducts three types of reviews. Full compliance reviews are conducted when an office has not been reviewed within the past 5 years. Follow-up reviews are conducted within 2 to 3 years of a full compliance review and are usually much shorter and less invasive. Advice and assist reviews are conducted at the request of a specific office or a component Security Programs Manager to provide advice or assistance with a particular security concern or issue. Table 11 lists the reviews conducted in FY 2010 and FY 2011, Quarter 1.

**Table 11: Compliance Review Team Reviews,
FY 2010 through FY 2011, Quarter 1**

Subject of Review	FY 2010			FY 2011, Qtr. 1	
	Advice and Assist	Follow-Up	Full	Follow-Up	Full
ATF		5	2	1	
DEA		5	3		
Executive Office of Immigration Review			2		
FBI			7		
Foreign Claims Settlement Commission			1		
DOJ Headquarters					1
Office for Victims of Crime			1		
Office of Information Policy			1		
Office of Juvenile Justice and Delinquency Prevention			1		
Office of Legislative Affairs					1
Office of Professional Responsibility					1
Office of the Solicitor General					1
USAOs		1	3		1
USMS	1	1	6		2
U.S. Trustees Office		1	4		1
Total	1	13	31	1	8

APPENDIX IX: BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES RESPONSE TO DRAFT REPORT



U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Office of the Director

Washington, DC 20226

JUN 29 2012

Michael E. Horowitz
Inspector General
U.S. Department of Justice
Office of the Inspector General
950 Pennsylvania Avenue, N.W.
Suite 4706
Washington, D.C. 20530-0001

Dear Mr. Horowitz:

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) appreciates the opportunity to respond to the recommendations from the Office of the Inspector General's report entitled, "The Department's and Components' Personnel Security Processes." ATF provides the following responses to Recommendation Numbers 11 and 12.

Recommendation Number 11: The components develop and implement procedures to ensure the field offices have access to headquarters' security information.

Response: ATF concurs with this recommendation. ATF acquired the Justice Security Tracking and Adjudication Record System (JSTARS) in October 2011. ATF's personnel security staff is currently modifying internal procedures and adapting to JSTARS processing activities and methods. It is intended that ATF's Division Operations Officers, Special Security Officers, Human Resources Specialists, and most Contracting Officers' Technical Representatives will have access to security information as "guest" role users in JSTARS. This is planned to be completed during Fiscal Year 2013.

Recommendation Number 12: The components require each field office to know the type of clearance each employee holds on site.

Response: ATF concurs with this recommendation. JSTARS has the capability to provide reports at the division level; however, due to a JSTARS coding error, ATF's Office of Professional Responsibility and Security Operations' Personnel Security Branch is currently prevented from generating quarterly reports for distribution to directorate and division offices. The JSTARS program office recognizes the issue and is actively working to correct the problem.

Michael E. Horowitz
Inspector General

Once resolved, the Personnel Security Branch will begin generating quarterly reports to distribute to division offices. It is anticipated that this will be favorably resolved and implemented by October 1, 2012.

Should you have any questions regarding this response, please contact Assistant Director Julie Torres, Office of Professional Responsibility and Security Operations at (202) 648-7500.

Sincerely,

A handwritten signature in black ink, appearing to read "B. Todd Jones". The signature is fluid and cursive, with a large loop at the end of the last name.

B. Todd Jones
Acting Director

**APPENDIX X: OIG ANALYSIS OF THE BUREAU OF ALCOHOL,
TOBACCO, FIREARMS AND EXPLOSIVES RESPONSE**

The Office of the Inspector General provided a draft of this report to the Bureau of Alcohol, Tobacco, Firearms and Explosives for its comment. ATF's response is included in Appendix IX to this report. The OIG's analysis of ATF's response and the actions necessary to close the recommendations are discussed below.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Status: Resolved.

ATF Response: ATF concurred with this recommendation. ATF's personnel security staff is currently modifying internal procedures and adapting its Justice Security Tracking and Adjudication Record System's (JSTARS) processing activities and methods to provide access to Division Operations Officers, Special Security Officers, Human Resources Specialists, and most Contracting Officers' Technical Representatives as "guest" role users in FY 2013.

OIG Analysis: ATF's actions are responsive to our recommendation. By October 15, 2012, please provide screenshots showing that ATF employees in the field have access as "guest" users, a copy of the reports provided to the field, and verification of JSTARS deployment to the field.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

ATF Response: ATF concurred with this recommendation. JSTARS has the capability to provide reports at the division level. However, due to a JSTARS coding error, ATF's Office of Professional Responsibility and its Security Operations' Personnel Security Branch cannot generate quarterly reports for directorate and division offices. The JSTARS program office is working to correct the problem. Once the problem is resolved, the Personnel Security Branch will distribute quarterly reports to division offices. ATF expected that this would be accomplished by October 1, 2012.

OIG Analysis: ATF's actions are responsive to our recommendation. Please provide confirmation that the JSTARS coding error has been resolved and that the Personnel Security Branch is distributing quarterly reports to the directorate and division offices by October 15, 2012. Please include documents showing the types of information that will be included in these reports.

**APPENDIX XI: THE FEDERAL BUREAU OF PRISONS RESPONSE TO
DRAFT REPORT**



U.S. Department of Justice

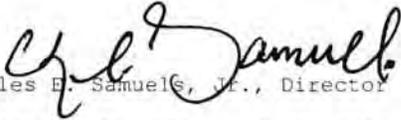
Federal Bureau of Prisons

Office of the Director

Washington, DC 20534

July 9, 2012

MEMORANDUM FOR MICHAEL D. GULLEDGE
ASSISTANT INSPECTOR GENERAL
FOR EVALUATION AND INSPECTIONS DIVISION

FROM:  Charles E. Samuel, Jr., Director

SUBJECT: Response to the Office of Inspector General's (OIG)
Draft Report: The Department's and Components'
Personnel Security Processes, Assignment Number
A-2011-002

The Bureau of Prisons (BOP) appreciates the opportunity to respond to the open recommendations from the draft report entitled The Department's and Components' Personnel Security Processes, Assignment Number A-2011-002.

Please find the Bureau's response to the recommendations below:

Recommendation #5: "To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that: the BOP work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases."

Response: The BOP agrees with the recommendation. The BOP has increased the number of staff in the Security Background Investigation Section, which has case review and adjudication responsibilities. Additionally, to improve timeliness of adjudications, when issues remain unresolved after due process,

Notification/Decision letters will be sent to the responsible Chief Executive Officer for administrative action or retention decision within 90 days.

Recommendation #10: "To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that: SEPS ensure that only the BOP Security Programs Manager authorize pre-employment waivers, as prescribed in the SEPS delegation of authority memorandum."

Response: The BOP agrees with the recommendation. The BOP is implementing procedures to ensure all pre-employment waivers are authorized by the BOP Security Program Manager prior to the end of FY 2012. Additionally, this will be assisted with the implementation of JSTARS.

Recommendation #11: "To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that: the components develop and implement procedures to ensure field offices have access to headquarters security information."

Response: The BOP agrees with the recommendation. Each field Human Resource Management (HRM) Office is notified when staff at their facility have security clearances added or changed in order to ensure Position Sensitivity Codes are changed in the database. Additionally, as part of the National Security Information (NSI) clearance review, each field office is notified annually of all staff in their facility who hold a "Secret" or "Top Secret" security clearance.

Recommendation #12: "To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that: the components require each field office to know the type of clearance each employee holds on site."

Response: The BOP agrees with the recommendation. Each field HRM Office is notified when staff at their facility have security clearances added or changed in order to ensure Position Sensitivity Codes are reflected appropriately within the NFC database. As part of the NSI clearance review, each field office is notified annually

of all staff in their facility with a "Secret" or "Top Secret" security clearance.

Recommendation #13: "To improve the Department's timeliness in processing background investigations and adjudications and to ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, we recommend that: the Department require components to track and report reciprocity data."

Response: The BOP agrees with the recommendation. The BOP will meet the requirements established by the Department of Justice.

If you have any questions regarding this response, please contact H. J. Marberry, Assistant Director, Program Review Division, at (202) 353-2302.

APPENDIX XII: OIG ANALYSIS OF THE FEDERAL BUREAU OF PRISONS RESPONSE

The Office of the Inspector General provided a draft of this report to the Federal Bureau of Prisons for its comment. The BOP's response is included in Appendix XI to this report. The OIG's analysis of the BOP's response and the actions necessary to close the recommendations are discussed below.

Recommendation 5: The BOP work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases.

Status: Resolved.

BOP Response: The BOP concurred with the recommendation. The BOP has increased the number of staff in the Security Background Investigation Section, which has case review and adjudication responsibilities. Additionally, to improve timeliness of adjudications, when issues remain unresolved after due process, Notification/Decision letters will be sent to the responsible Chief Executive Officer for administrative action or retention decision within 90 days.

OIG Analysis: The BOP's actions are responsive to our recommendation. By October 15, 2012, please provide documentation that reflects the staffing level before and after the increase to the Security Background Investigation Section. Please also provide documentation to show that decision letters for unresolved issues are sent within 90 days after due process.

Recommendation 10: SEPS ensure that only the BOP Security Programs Manager authorize pre-employment waivers as prescribed in the SEPS delegation of authority memorandum.

Status: Resolved.

BOP Response: The BOP concurred with the recommendation. The BOP is implementing procedures to ensure all pre-employment waivers are authorized by the BOP Security Program Manager prior to the end of FY 2012. The change in procedures will be assisted by the implementation of JSTARS.

OIG Analysis: The BOP's planned actions are responsive to our recommendation. Please provide a copy of the new procedures that verify

pre-employment waiver authorizations are signed by the security managers and verification of the JSTARS deployment, by October 15, 2012.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Status: Resolved.

BOP Response: The BOP concurred with the recommendation. Each field Human Resource Management (HRM) Office is notified when staff at that facility has security clearances added or changed in order to ensure Position Sensitivity Codes are changed in the database. Additionally, as part of the National Security Information (NSI) clearance review, each field office is notified annually of all staff in the facility that hold a "Secret" or "Top Secret" security clearance.

OIG Analysis: The BOP's actions are responsive to our recommendation. By October 15, 2012, please provide verification that each HRM Office has access to headquarters security information and provide documentation that all facilities received the annual notification of staff clearance levels.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

BOP Response: The BOP concurred with the recommendation. Each field HRM Office is notified when staff at their facility has security clearances added or changed in order to ensure Position Sensitivity Codes are reflected appropriately within the National Finance Center database. As part of the NSI clearance review, each field office is notified annually of all staff in their facility with a "Secret" or "Top Secret" security clearance.

OIG Analysis: The BOP's actions are responsive to our recommendation. Please provide documentation that all facilities received the annual notification staff's clearance levels By October 15, 2012.

Recommendation 13: The Department require components to track and report reciprocity data.

Status: Closed.

BOP Response: The BOP concurred with the recommendation. The BOP will meet the requirements established by the Department of Justice.

OIG Analysis: In response to our recommendation, which was directed to the Department, the BOP agreed to follow established reciprocity tracking and reporting requirements and should coordinate with SEPS on all related actions. No further status reports are required from the BOP on Recommendation 13.

APPENDIX XIII: THE DRUG ENFORCEMENT ADMINISTRATION RESPONSE TO DRAFT REPORT



U. S. Department of Justice
Drug Enforcement Administration

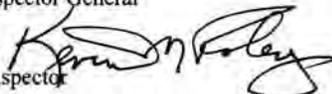
www.dea.gov

Washington, D.C. 20537

JUL - 3 2012

MEMORANDUM

TO: Michael D. Gulledge
Assistant Inspector General
for Evaluation and Inspections
Office of the Inspector General

FROM: Kevin M. Foley 
Deputy Chief Inspector
Office of Inspections

SUBJECT: DEA's Response to the OIG's Draft Report: *Review of the Department's and Components' Personnel Security Process, A-2011-002*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ), Office of the Inspector General's (OIG) draft report, entitled: *Review of the Department's and Components' Personnel Security Process, A-2011-002*. DEA acknowledges OIG's efforts in conducting a thorough review of the management of the personnel security process at DOJ and its components. As a result of this review, DEA concurs with the two recommendations directed to the DOJ components in the draft report and has taken the necessary steps to implement the recommendations.

OIG's recommendations 1 – 10 and 13 were directed to the Department; therefore, DEA provides the following responses to the OIG's recommendations 11 and 12 directed to the components:

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

DEA Response: DEA concurs and has taken proactive steps to accomplish this recommendation. As a result of the implementation of the Justice Security Tracking and Adjudication Record System (JSTARS), the Office of Security Programs, Personnel Security Section (ISR) implemented requirements for DEA domestic offices and foreign regions. The Offices must submit updated quarterly divisional rosters of employees, contractors, linguists, Task Force Officers (TFOs), and employees under a Personnel Service Agreement who have authorized access to DEA facilities and/or DEA Information Technology systems, by virtue of favorable background investigations and granting of appropriate clearance/access. ISR provides

each Division Security Officer (DSO) with an electronic spreadsheet to promote the uniform submission of the quarterly divisional rosters. The quarterly divisional roster is a spreadsheet that contains identifying information, position/job title, and badge/credential information. ISR reviews each roster to verify the accuracy of the data in JSTARS and directly corresponds with DSOs to confirm the accuracy of the rosters and/or requests of the DSOs for an appropriate security package to be updated or submitted. In doing so, field offices have a timely and accurate account of each individual entering DEA facilities. In the event a security issue arises that necessitates immediate headquarters attention, each DSO has a designated point of contact within ISR to address these security matters.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

DEA Response: DEA concurs and has taken proactive steps to accomplish this recommendation. As a result of the implementation of JSTARS, ISR implemented requirements of each DSO to maintain a current divisional roster, which documents the fluidity of the labor force within each DEA facility. Once a favorable adjudication and review is determined by ISR and reported to JSTARS, JSTARS automatically forwards a Certification of Investigation to the DSO and DEA employee of the type of clearance each DEA employee holds. In the case of contractors and TFOs, JSTARS automatically forwards a TFO/Contractor Approval Letter to the DSO of the type of clearance/access each contractor holds. These notices are maintained by the DSO.

Based on the information provided, DEA requests closure of recommendations 11 and 12. If you have any questions regarding DEA's response to the OIG's recommendations, please contact the Audit Liaison Team at (202) 307-8200.

APPENDIX XIV: OIG ANALYSIS OF THE DRUG ENFORCEMENT ADMINISTRATION RESPONSE

The Office of the Inspector General provided a draft of this report to the Drug Enforcement Administration for its comment. The DEA's response is included in Appendix XIII to this report. The OIG's analysis of the DEA's response and the actions necessary to close the recommendations are discussed below.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Status: Resolved.

DEA Response: The DEA concurred with this recommendation. As a result of implementing JSTARS, the Office of Security Programs, Personnel Security Section (ISR), implemented requirements for DEA domestic offices and foreign regions. Those offices must submit updated quarterly divisional rosters of employees, contractors, linguists, Task Force Officers (TFO), and employees under a Personnel Service Agreement who have authorized access to DEA facilities or DEA information technology systems.

ISR provides each Division Security Officer (DSO) with an electronic spreadsheet to promote the uniform submission of the rosters. The roster contains identifying information, position/job title, and badge/credential information. ISR reviews each roster to verify the accuracy of the data in JSTARS and directly corresponds with DSOs to confirm the accuracy of the rosters or requests DSOs update or submit an appropriate security package. This provides field offices with a timely and accurate account of each individual entering DEA facilities. If a security issue arises that necessitates immediate headquarters attention, each DSO has a designated point of contact within ISR to address these security matters.

OIG Analysis: The actions taken by the DEA are responsive to our recommendation. By October 15, 2012, please provide a copy of the template that DSOs will use to report the security information of employees, contractors, linguists, TFOs, and other employees in their divisions, and a copy of the policies, memoranda, or other documentation requiring the DSOs to submit this information on a quarterly basis.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

DEA Response: The DEA concurred with this recommendation. As a result of implementing JSTARS, ISR implemented requirements that each DSO maintain a current divisional roster that documents the fluidity of the labor force within each DEA facility. Once a favorable adjudication and review is determined by ISR and reported to JSTARS, JSTARS automatically forwards a Certification of Investigation to the DSO and DEA employee of the type of clearance each DEA employee holds. In the case of contractors and TFOs, JSTARS automatically forwards a TFO/Contractor Approval Letter to the DSO of the type of clearance/access each contractor holds. These notices are maintained by the DSO.

OIG Analysis: The actions taken by the DEA are responsive to our recommendation. Please provide a copy of a Certificate of Investigation and an Approval Letter as documentation that these actions have been completed by October 15, 2012.

APPENDIX XV: THE FEDERAL BUREAU OF INVESTIGATION RESPONSE TO DRAFT REPORT



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 9, 2012

The Honorable Michael E. Horowitz
Inspector General
U.S. Department of Justice
Office of the Inspector General
950 Pennsylvania Avenue, Northwest
Washington, D.C. 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your report entitled, "The Department's and Components' Personnel Security Processes" (hereinafter, "Report").

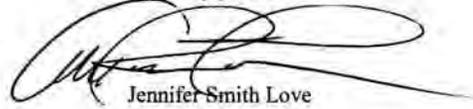
We are pleased you determined that during the period of the review the Department was able to recruit and retain qualified individuals to meet mission critical needs. As demonstrated to your auditors, the FBI exceeded its hiring goals for Special Agents (SA) and Intelligence Analysts (IA) in fiscal year 2010 successfully placing 914 SAs and 594 IAs throughout our nation at multiple FBI Field Offices and FBI Headquarters.

While we continually strive to improve the timeliness of our clearance process, the complexities and intricacies of completing a Top Secret (TS) National Security Information clearance should not be understated. As your Report concludes, the FBI averaged only eight days to adjudicate backgrounds with the bulk of time being expended on conducting the actual Background Investigation (BI). It also bears noting the FBI has discussed with the Office of the Directorate of National Intelligence (ODNI) the differences in completing a BI for a Secret versus TS clearance. Based upon these discussions, it is our understanding ODNI is currently studying the guidelines issued by the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) and will likely issue revised guidelines for TS clearances.

Based upon a review of the Report, the FBI concurs with your recommendations. The FBI appreciates the professionalism exhibited by your staff to complete this audit. Enclosed herein is the FBI's response to the recommendations directed towards the FBI. Please feel free to

contact me should you have any questions.

Sincerely yours,



Jennifer Smith Love
Assistant Director
Security Division

Enclosure

UNCLASSIFIED

**Department of Justice Office of Inspector General
The Department's and Components' Personnel Security Processes**

Recommendation #11: "The components develop and implement procedures to ensure field offices have access to headquarters' security information."

FBI Response: Concur - The FBI will ensure that field offices have access to headquarters security information (not subject to privacy act), through the following systems:

- FBI Employees – Bureau Personnel Management System (BPMS);
- Non-FBI Employees (excluding DOJ) – Facility Security System (FSS); and,
- DOJ Employees, FBI Employees, and non-FBI Employees – Justice Security Tracking and Adjudication Records System (JSTARS)

The Chief Security Officers (CSO) are aware, and will be advised again, that the security information required to determine access to FBI space and information systems is available in these systems.

Recommendation #12: "The components require each field office to know the type of clearance each employee holds on site."

FBI Response: Concur – Through the use of the systems noted in response to Recommendation #11, each FBI field office will know the clearance level and type of clearance for each individual (FBI employee and non-FBI employee) with access to FBI space and information systems. The FBI will ensure each field office receives the necessary training to operate each system. This will be accomplished through notification and training of the CSOs for each field office.

Recommendation #13: "The Department require components to track and report reciprocity data."

FBI Response: Concur - The FBI will track and report cases processed under reciprocity policy and guidelines as required by the Office of Directorate on National Intelligence (ODNI). The FBI will accomplish this using the FBI's Clearance Processing System (CPS).

UNCLASSIFIED

APPENDIX XVI: OIG ANALYSIS OF THE FEDERAL BUREAU OF INVESTIGATION RESPONSE

The Office of the Inspector General provided a draft of this report to the Federal Bureau of Investigation for its comment. The FBI's response is included in Appendix XV to this report. The OIG's analysis of the FBI's response and the actions necessary to close the recommendations are discussed below.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Status: Resolved.

FBI Response: The FBI concurred with this recommendation. The FBI stated that it will ensure that field offices have access to headquarters security information (not subject to the *Privacy Act*), through the following systems:

- FBI employees – Bureau Personnel Management System (BPMS);
- Non-FBI employees (excluding DOJ employees) – Facility Security System (FSS); and
- DOJ employees, FBI employees, and non-FBI employees – JSTARS.

The Chief Security Officers (CSO) have been advised, and will be advised again, that the security information required to determine access to FBI space and information systems is available in these systems.

OIG Analysis: The FBI's actions are responsive to our recommendation. Please provide documentation to verify CSOs have access to headquarters' security information by October 15, 2012.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

FBI Response: The FBI concurred with this recommendation. Through the use of the systems noted in response to Recommendation 11, each FBI field office will know the clearance level and type of clearance for each individual (FBI employee and non-FBI

employee) with access to FBI space and information systems. The FBI stated that it will ensure each field office receives the necessary training to operate each system. This will be accomplished through notification and training of the CSOs for each field office.

OIG Analysis: The FBI's planned actions are responsive to our recommendation. Please provide documentation that FBI field offices can verify employees' security clearance and access levels by October 15, 2012.

Recommendation 13: The Department require components to track and report reciprocity data.

Status: Closed.

FBI Response: The FBI concurred with this recommendation. The FBI stated that it will track and report cases processed under reciprocity policy and guidelines as required by the Office of the Director of National Intelligence. The FBI stated that it will accomplish this using its Clearance Processing System.

OIG Analysis: In response to our recommendation, which was directed to the Department, the FBI agreed to follow established reciprocity tracking and reporting requirements and should coordinate with SEPS on all related actions. No further status reports are required from the FBI on Recommendation 13.

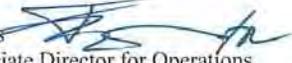
**APPENDIX XVII: THE U.S. MARSHALS SERVICE RESPONSE TO
DRAFT REPORT**



U.S. Department of Justice
United States Marshals Service
Associate Director for Operations

Alexandria, Virginia 22301-1025
July 9, 2012

MEMORANDUM TO: Michael D. Gulledge
Assistant Inspector General
for Evaluation and Inspection

FROM: Eben Morales 
Acting Associate Director for Operations

SUBJECT: USMS Comments on Review of the Department's and
Component's Personnel Security Process, Report Number
A-2011-002

This is in response to your recent memorandum dated June 20, 2012, regarding the subject report.

Should you have any questions regarding this response, please contact Ms. Isabel Howell at 202-307-9744.

Attachments

cc: William D. Snelson
Assistant Director
Tactical Operations Division

Donald O'Hearn
Chief of Staff

Isabel Howell
External Audit Liaison Team
United States Marshals Service

Louise Duhamel
Acting Director, Audit Liaison Group
Justice Management Division

Mary T. Myers
Audit Liaison Specialist, Audit Liaison Group
Justice Management Division

USMS Comments on Recommendations
The Department's and Components' Personnel Security Processes
Report Number A-2011-002

Recommendation 11 (Concur): The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Recommendation 12 (Concur): The components require each field office to know the type of clearance each employee holds on site.

USMS Response: The United States Marshals Service (USMS) concurs with both Recommendations 11 and 12 and has taken steps to ensure that district field office personnel can more readily obtain personnel security information.

First, background investigations are processed and adjudicated by the Office of Security Programs (OSP) at USMS Headquarters. OSP staff maintains and tracks security information in the Justice Security Tracking and Adjudication Record System (JSTARS) and Marshals Workforce Information System/Exchange (M-WISE). District field offices have access to the M-WISE system. Chief Deputy United States Marshals (Chiefs) and district Administrative Officers (AOs) can view background data for their district personnel through M-WISE. OSP is working with M-WISE staff to grant the Chiefs and AOs additional M-WISE access, which would include the Investigation Report. In addition, each employee can view his or her personal information page on M-WISE, which includes information such as clearance level and reinvestigation due date.

Second, every district has a District Security Program Officer (DSPO) who serves as a liaison between the district and Headquarters regarding security matters. The DSPO is responsible to the Agency Security Program Manager for implementation and administration of security programs as delegated and assigned. One primary duty involves maintaining a current list of employee clearance levels and a centralized database for reinvestigations at Headquarters, in addition to other security-related duties. The USMS intends to encourage the DSPOs to maintain a regular dialogue with Headquarters to ensure that personnel security information is available to the Districts.

Further, OSP staff is readily available to provide direction and information to district field offices. Employees are advised at the conclusion of their five-year reinvestigation of clearance level and next reinvestigation due date. In addition, prior to each fiscal year, OSP generates and maintains a master list of all employees requiring a reinvestigation for the upcoming fiscal year.

Finally, we strive for open communication and transparency. Guidance on security matters is posted on the USMS Intranet, reiterated throughout the year in training, and detailed in Agency policy.

APPENDIX XVIII: OIG ANALYSIS OF THE U.S. MARSHALS SERVICE RESPONSE

The Office of the Inspector General provided a draft of this report to the U.S. Marshals Service for its comment. The USMS's response is included in Appendix XVII to this report. The OIG's analysis of the USMS's response and the actions necessary to close the recommendations are discussed below.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

Status: Resolved.

USMS Response: The USMS concurred with this recommendation. The USMS stated that it has taken steps to ensure that district field office personnel can more readily obtain personnel security information. Background investigations are processed and adjudicated by the Office of Security Programs (OSP) at USMS headquarters. The OSP staff maintains and tracks security information in JSTARS and the Marshals Workforce Information System/Exchange (M-WISE). District field offices have access to the M-WISE system. Chief Deputy U.S. Marshals (Chiefs) and district Administrative Officers (AO) can view background data for their district personnel through M-WISE. OSP is working with M-WISE staff to grant the Chiefs and AOs additional M-WISE access, which would include the Investigation Report. In addition, each employee can view his or her personal information page on M-WISE, which includes information such as clearance level and reinvestigation due date.

Further, the USMS stated that the OSP staff is readily available to provide direction and information to district field offices. Employees are advised at the conclusion of their 5-year reinvestigation of their clearance level and next reinvestigation due date. In addition, prior to each fiscal year, OSP generates and maintains a master list of all employees requiring a reinvestigation in the upcoming fiscal year.

OIG Analysis: The actions taken by the USMS are responsive to our recommendation. However, we believe that the district field offices should be aware of when their employees are due for a reinvestigation and that this information should not be limited to headquarters. By October 15, 2012, please provide screenshots showing the specific M-WISE data fields and reports that district field offices are able to

access, as well as a description of how OSP plans to share information regarding employee reinvestigations with the field. Also please provide verification that District Security Program Officers (DSPO) are aware of the periodic reinvestigation date for each employee in their districts.

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

USMS Response: The USMS concurred with this recommendation. Every district has a DSPO who serves as a liaison between the district and headquarters on security matters. The DSPO is responsible to the Agency Security Program Manager for implementation and administration of security programs as delegated and assigned. One primary duty involves maintaining a current list of employee clearance levels and a centralized database for reinvestigations at headquarters, in addition to other security-related duties. The USMS stated that it intends to encourage the DSPOs to maintain a regular dialogue with headquarters to ensure that personnel security information is available to the districts.

OIG Analysis: The actions taken by the USMS are responsive to our recommendation. Please provide a copy of the USMS policy documents describing the DSPO's requirement to maintain a current list of employee clearance levels by October 15, 2012. In addition, please provide documentation showing how the USMS intends to facilitate communication between headquarters and the DSPOs.

APPENDIX XIX: THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE TO DRAFT REPORT



U.S. Department of Justice

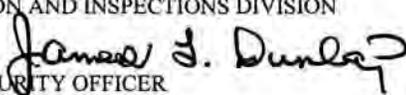
Justice Management Division

Security and Emergency Planning Staff

Washington, D.C. 20530

JUN 29 2012

TO: MICHAEL D. GULLEDGE
ASSISTANT INSPECTOR GENERAL
FOR EVALUATION AND INSPECTIONS DIVISION

FROM: JAMES L. DUNLAP 
DEPARTMENT SECURITY OFFICER

SUBJECT: Response to OIG's Report Entitled: *Review of the Department's and
Component's Personnel Security Processes, Assignment Number A-2011-002*

This responds to the OIG's report entitled: *Review of the Department's and Component's
Personnel Security Processes, Assignment Number A-2011-002.*

I welcome and appreciate this review regarding the personnel security process in the Department. The OIG staff was very thorough and their professionalism was greatly appreciated. As requested, I will address the reports's recommendations and provide the appropriate plan of action for each recommendation. I would like to take this opportunity to highlight some concerns we have regarding this report, and I provide them below for the permanent record.

The methodology used in the review and presented in the Draft combines both the investigative timeliness and adjudicative timeliness elements. With the exception of the Federal Bureau of Investigation (FBI) and the Alcohol, Tobacco, Firearms and Explosives (ATF), the Department is *only* held accountable for achieving the adjudicative timeliness element required in the 2004 Intelligence and Terrorism Prevention Act (IRTPA). All other Department components utilize the U.S. Office of Personnel Management (OPM) and, therefore, are not accountable for OPM's investigative timeliness. Progress reports received from the Office of the Director of National Intelligence (ODNI), the entity responsible for ensuring government IRTPA compliance, clearly indicate this fact. The ODNI reports state that OPM is responsible for the investigative timeliness for the non FBI/ATF reports. In this Draft, *the OIG acknowledges that the Department met the 20-day guideline for adjudication, averaging 16 days for that phase of the process.* It is our concern that the OIG, in this report is holding the Department to different standards than the ODNI expects from the DOJ. The fact that the review shows that the Department's adjudication timeliness averages 16 days should be celebrated; not buried within the report.

The OIG utilized data from this review from FY 2010 and 1st Quarter of FY 2011. This is a concern because the current reports from OPM and the ODNI show much improvement; making the OIG findings regarding the Department's timelines obsolete. The Security and Emergency

Subject: Response to OIG's Report Entitled: Review of the Department's and Component's Personnel Security Processes, Assignment Number A-2011-002

Planning Staff (SEPS) continues to make IRTPA adjudication timeliness one of its priorities and monitors components' progress on a monthly basis. SEPS is closely working with the few components who struggle to meet the adjudicative timeliness to bring them to compliance.

The OIG report indicates that "...Department excludes attorney positions from its timeliness reports. As a result Department managers, and OPM, lacked information that would have alerted them to inefficiencies or delays in the non-FBI attorney clearance process." This statement is of concern in that the "exclusion" was not intentional, but rather has been and continues to be a technical issue within the OPM's personnel security system. The DOJ SEPS staff has been aware of this issue and has worked to address it several times. We are once again, engaged with OPM and were recently notified by OPM that their IT system redesign is in progress, with an anticipated completion of the first quarter of FY 2013.

The final item I would like to address is the report's statement about Public Trust employees who are permitted to start work with a pre-employment waiver. The report states that as a result these individuals routinely work in the Department, with access to sensitive information and systems, for significant periods of time without the completed investigation and adjudication. The OIG report states that three percent of the employees had investigations and adjudications that took over a year to complete and therefore, exceeded the individual's probationary period.

This pre-employment waiver consists of a favorable review of the security form, favorable results of the fingerprints check, a check of government databases to ensure there is no current investigation meeting the scope of the position or an unfavorable investigation, and a favorable credit check. Any issues developed in these areas are addressed and resolved prior to the employee being approved to enter on duty. It is important to note that the extensive waiver approval process provides for an acceptable risk to allow these employees to begin work while the investigation is in process. The report did not address the reason why the three percent of Public Trust cases had not been completed. Upon discussion with the OIG, they stated that they did not find out the reason the investigations were not adjudicated. The OIG further clarified that they were just looking for completion of the process. Therefore, SEPS cannot address the three percent of cases not having been completed other than it is not inconceivable these individuals could have had activities in foreign countries or issues currently being addressed by the adjudicative office.

Many of the statements and recommendations mentioned in this review were already known and addressed by SEPS. For several years, SEPS has been developing a Department-wide personnel security tracking system, the Justice Security Tracking and Adjudication Record System (JSTARS), to address oversight inefficiencies previously identified by my staff. The timing of this review coincided with the last two years of the system's planned deployment to the Department components. Many of the items identified as issues will be fully resolved with the implementation of JSTARS. For example, the OIG report indicates that "Although components track data on the status of employee background investigations, clearance levels and reinvestigations, the tracking is inconsistent and often incomplete." This is fully addressed by the enterprise deployment of JSTARS; which gives the DOJ an effective oversight tool. Another example is the report's finding that the Department does not track reciprocal acceptance of

security clearances. JSTARS was built with this functionality in mind and since its inception in July 2008, it has had this capability. However, since JSTARS was not fully deployed to all Departmental personnel security offices; not all components had this capability.

I believe the recommendations from this report will have a positive impact in our personnel security and compliance review programs. The OIG report contains 13 recommendations. Information below responds to the recommendations. The recommendation numbers correspond to those in the OIG report.

1. OARM should work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals.

We concur with this recommendation. Both SEPS and OARM have already held two meetings (January 17, 2012 and February 6, 2012) to re-engineer the review process between the two offices. The Department's Personnel Security System, JSTARS will need to be changed to accommodate the new process.

Next Steps:

- Hold meeting with SEPS, OARM and JSTARS Development team to identify requirements for the new Attorney review process. Meeting is scheduled for July 10, 2012.
- JSTARS team develops new process; specialists will test new process and concur with the new development.
- New process is deployed to JSTARS.
- Estimated completion time is three months from requirements gathering phase, approximately on November 2, 2012.

2. OARM should reduce the time-limited appointment waiver period from 18 months to 12 months and 1 day to complete suitability determinations.

OARM is responsible for replying to this recommendation.

3. OARM should increase the amount of staff dedicated to processing completed investigations.

OARM is responsible for replying to this recommendation.

4. SEPS should work with OPM, FBI and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's IRTPA timeliness reports.

SEPS concurs with this recommendation, but the successful implementation of this recommendation is dependent on OPM's technology improvements. SEPS has already communicated to the FBI that all attorney and political appointee investigations are to be

expedited. SEPS has held several discussions with OPM representatives to address the IT impediment and OPM has recently stated they would not be able to accommodate this request until their IT system is redesigned. (Estimated time of completion is the 1st Quarter of FY 2013.)

5. The BOP should work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases.

SEPS concurs with this recommendation; however, believes that the timeliness requirement has already been properly communicated through DOJ Order 2610.2B which already states that Public Trust investigations must be adjudicated within 90 days of completion. SEPS will remind BOP of this timeliness requirement via memorandum from the Department Security Officer.

Estimated Date: July 30, 2012

6. SEPS should work with components to ensure that approvals for individuals in a probationary status are completed prior to the end of the probation period.

As mentioned above, DOJ Order 2610.2B addresses the timeliness requirement for Public Trust adjudications. SEPS will remind components of the importance of meeting this deadline and its impact on probationary status employees via memorandum from the Department Security Officer.

Estimated Date: July 30, 2012

7. The Department should require components to share internal review results with SEPS.

SEPS agrees with this recommendation. On June 8, 2012, SEPS sent a data call to DOJ components soliciting copies of their internal audit and inspection reports to leverage limited resources and reduce duplication of oversight efforts with the Department.

Additionally, a policy statement will be sent to component Security Programs Managers requiring components share internal security review results with SEPS.

Estimated Date: September 30, 2012

8. The Compliance Review Team should use the results of components' internal reviews to identify trends and recurring personnel security problems across the Department and focus on the most critical security issues.

SEPS agrees with this recommendation and will communicate the request to all Department components.

On June 8, 2012, SEPS sent a data call request to DOJ components soliciting copies of their internal information, combined with the required annual component security self-inspections. The self-inspection results will be utilized to analyze trends and recurring personnel security deficiencies. The information will also be utilized to create security

education and awareness tools to enhance the Department's Security Programs.

Estimated Date: December 30, 2012

9. SEPS should increase the amount of staff dedicated to conducting compliance reviews.

SEPS concurs with this recommendation. Due to today's fiscally conservative environment and the current hiring freeze impacting the Department, SEPS cannot guarantee it will be able to hire additional full time employees. SEPS has already re-engineered its human capital resources for maximum effectiveness given the existing budget. However, we will continue to look for opportunities to re-program critical resources and personnel to ensure the Department has an effective security compliance review program.

10. SEPS should ensure that only the BOP Security Programs Manager authorize pre-employment waivers, based on the SEPS delegation of authority memorandum.

SEPS concurs with this recommendation and is already engaged with BOP to achieve this recommendation. On March 26, 2012, the DSO communicated to BOP's SPM the fact that BOP needed to ensure compliance with the March 20, 2003 delegation of authority memorandum by June 1, 2012.

BOP responded in correspondence to the Deputy Assistant Attorney General for Human Resources and Administration (DAAG/HRA) April 20, 2012, requesting postponement of the due date given complexities in this request.

Via memorandum dated April 30, 2012, the DAAG/HRA requested from BOP an implementation plan.

On June 1, 2012, BOP communicated an implementation plan which would bring BOP into compliance with its delegated authority by August 2012.

On June 13, 2012 BOP personnel met with SEPS personnel to discuss JSTARS deployment strategy for BOP.

BOP personnel have stated they will make their deployment decision by end of June, 2012.

BOP's utilization of JSTARS will ensure their pre-employment waivers are reviewed by their security staff before their employees and contractors commence work.

11. The components develop and implement procedures to ensure field offices have access to headquarters' security information.

12. The components require each field office to know the type of clearance each employee holds on site.

Recommendations 11 and 12 above would be covered if all components choose to provide their field offices access to JSTARS or provide them with monthly reports.

Subject: Response to OIG's Report Entitled: Review of the Department's and Component's Personnel Security Processes, Assignment Number A-2011-002

SEPS has provided this tool through JSTARS and has recommended the practice to all components. To date, only the Executive Office for U.S. Attorneys has chosen to utilize this functionality.

The DSO will remind all Security Programs Managers of this functionality within JSTARS by August 1, 2012, and request that they share information with their respective field offices.

13. The Department require components to track and report reciprocity data.

Everyone utilizing JSTARS will be compliant with this recommendation as the system was built with this functionality. SEPS has been able to track this information since the system's inception on July 21, 2008.

SEPS is committed to a strong and effective personnel security program, and recognizes that there is always room for improvement. Therefore, you have my commitment that SEPS will work diligently to implement the recommendations to the best of its ability as quickly as possible. Should you have any questions or require additional information, please contact me directly at (202) 514-2094 or Dorianna Rice, Assistant Director, Personnel Security Group, at (202) 514-2351.

APPENDIX XX: OIG ANALYSIS OF THE SECURITY AND EMERGENCY PLANNING STAFF RESPONSE

The Office of the Inspector General provided a draft of this report to the Justice Management Division's Security and Emergency Planning Staff for its comment. SEPS's response is included in Appendix XIX to this report. The OIG's analysis of SEPS's response and the actions necessary to close the recommendations are discussed below.

GENERAL COMMENTS

We agree with SEPS that not all components are responsible for each part of the security clearance process, and for this reason our report does not assign blame to the Department or SEPS for the lengthy periods taken to conduct background investigations. However, as discussed in multiple conversations with SEPS officials, the OIG is evaluating the entire security clearance process, including both background investigations and adjudications, and that evaluation requires presenting a complete picture of the time it takes to complete the entire process for DOJ employees.

SEPS's response expresses concern that the data used for the report is obsolete, and the response cites recent ODNI and OPM data that indicates improvement in the timeliness of the Department's adjudications. The data the OIG used was the most current complete data available at the start of the review. Moreover, our report acknowledges at the outset that the Department met the IRTPA standard for adjudication, which is an important element of the overall security clearance process. However, unlike ODNI's and OPM's assessments, the OIG's review assesses the entire process, not just the adjudication element, and for that reason among others we strongly disagree that the data we used is obsolete.

SEPS's response also expresses the concern that the OIG has implied that SEPS intentionally excluded attorney data from Department timeliness reports, when according to the response these exclusions were instead due to ongoing technical issues with OPM that prohibited the inclusion of the data. We believe SEPS's response mischaracterizes our report. The report does not assert, nor do we intend to imply, that attorney data was intentionally excluded. Rather, the report properly notes that SEPS is ultimately responsible for ensuring that all data is reported.

SEPS's response also takes issue with our statement on page 40 that "it took more than one year to complete the background investigations and adjudications for 3 percent of the employees in Public Trust positions, which exceeded their one year probationary periods." The SEPS response states that "the extensive waiver approval process provides for an acceptable risk to allow these employees to begin work while the investigation is in process." Although the current procedures for completing pre-employment waivers consist of several checks conducted by HR personnel, the waivers are not always reviewed by security personnel prior to the individual starting work as we note on pages 39 and 45. As a result, the OIG is concerned that the potential for security risks exists, and for this reason we have highlighted the issue in our report.⁶²

Finally, the OIG is aware that SEPS has been developing and implementing JSTARS. We agree that full implementation of JSTARS among all components should address many of the recommendations in this report.

RESPONSES TO RECOMMENDATIONS

Recommendation 1: OARM work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS and OARM held two meetings (on January 17, 2012, and February 6, 2012) to re-engineer the review process between the two offices. JSTARS, will need to be changed to accommodate the new process. SEPS stated that it expected to the following steps to be completed by approximately November 2, 2012:

- SEPS will meet with OARM and the JSTARS development team to identify system requirements for the new attorney review

⁶² We also disagree with the statement in SEPS's response that, because the OIG did not identify and evaluate the reason for the delays in the security clearance process for the employees in these Public Trust positions, "SEPS cannot address [these] cases." As stated in our report, SEPS is the primary office responsible for developing, implementing, and ensuring compliance with security policy throughout the Department, and it conducts oversight of the Department's personnel security processes. In light of those responsibilities, we believe SEPS is well positioned to identify and address the causes of these delays.

-
-
- process. The meeting was scheduled for July 10, 2012.
- The JSTARS team will develop a new process that will be tested by specialists before deployment.
 - The new process will be deployed to JSTARS.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide documentation of the completed process by January 15, 2013. If the process is not completed by that date, please provide a status update of the steps that have been completed and a new estimated completion date.

Recommendation 4: SEPS work with OPM, FBI and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's IRTPA timeliness reports.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation, but stated that the successful implementation of this recommendation depends on OPM's technology improvements. SEPS has already communicated to the FBI that all attorney and political appointee investigations are to be expedited. SEPS also has held several discussions with OPM representatives to address the information technology impediment, and OPM recently stated it would not be able to accommodate this request until its system is redesigned. According to SEPS, the redesign is expected to be completed in the first quarter of FY 2013.

OIG Analysis: SEPS's actions are partially responsive to our recommendation. SEPS and OPM have been aware of this issue for the past 2 years and have held several discussions and meetings. However, SEPS is still not reporting the Department attorney timeliness data. Although there are technical issues related to reporting attorney data, the requirement still exists. SEPS should explore alternative reporting methods and develop a written plan of action in the event that OPM's longstanding technical issues are not resolved. Please provide a copy of the alternative action plan for reporting attorney data by October 15, 2012. Additionally, please provide a detailed status report of any subsequent meetings with OPM, by January 15, 2013.

Recommendation 5: The BOP work with SEPS to establish procedures to improve its timeliness in adjudicating Public Trust cases.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. However, SEPS stated that the timeliness requirement has already been properly communicated through DOJ Order 2610.2B, which states that Public Trust investigations must be adjudicated within 90 days of completion. SEPS planned to remind the BOP of this timelines requirement via a memorandum from the Department Security Officer to be issued by the end of July 2012.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide a copy of the Department memorandum from the Department Security Officer to the BOP by October 15, 2012, and describe how SEPS will specifically work with the BOP to improve adjudication reporting timeliness.

Recommendation 6: SEPS work with components to ensure that approvals for individuals in a probationary status are completed prior to the end of the probation period.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS stated that it will remind components of the importance of meeting the deadline established by DOJ Order 2610.2B and its impact on probationary status employees via a memorandum from the Department Security Officer to be issued by the end of July 2012.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide a copy of the Department memorandum outlining the deadline requirements by October 15, 2012, along with documentation showing that SEPS can identify Department employees who are within 60 days of reaching permanent status and do not have a completed investigation.

Recommendation 7: The Department require components to share internal review results with SEPS.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. On June 8, 2012, SEPS sent a data call to DOJ components soliciting copies of their internal audit and inspection reports to leverage limited resources and reduce duplication of oversight efforts with the Department. Additionally, it planned to send a policy statement to component Security Programs Managers by the end of September 2012 requiring components share internal security review results with SEPS.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. By October 15, 2012, please provide a copy of the data call to DOJ components and a copy of the policy statement requiring components to share internal security results with SEPS. In addition, please provide documentation that component Security Programs Managers are sharing internal security review results with SEPS.

Recommendation 8: The Compliance Review Team use the results of components' internal reviews to identify trends and recurring personnel security problems across the Department and focus on the most critical security issues.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. On June 8, 2012, SEPS sent a data call to DOJ components soliciting copies of their internal information, combined with the required annual component security self-inspections. The self-inspection results will be used to analyze trends and recurring personnel security deficiencies. The information also will be used to create security education and awareness tools to enhance the Department's Security Programs. SEPS estimated that these steps would be completed by the end of December 2012.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide copies of inspection documents that reflect that the Compliance Review Team has incorporated trends discovered during internal component self-inspections into Department inspection procedures by January 15, 2013.

Recommendation 9: SEPS increase the amount of staff dedicated to conducting compliance reviews.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. Because of the current fiscal environment and the hiring freeze affecting the Department, SEPS stated that it cannot guarantee it will be able to hire additional full-time employees. SEPS stated that it had already re-engineered its human capital resources for maximum effectiveness given the existing budget. It also stated that it would continue to look for opportunities to re-program critical resources and personnel to ensure the Department has an effective security compliance review program.

OIG Analysis: SEPS's actions are responsive to our recommendation. Please provide documentation that reflects SEPS's re-engineered procedures to maximize Compliance Review Team resources by October 15, 2012.

Recommendation 10: SEPS ensure that only the BOP Security Programs Manager authorize pre-employment waivers as prescribed in the SEPS delegation of authority memorandum.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. On March 26, 2012, the Department Security Officer informed the BOP's SPM that, by June 1, 2012, the BOP needed to ensure compliance with the March 20, 2003, delegation of authority memorandum. The BOP requested an extension from the Deputy Assistant Attorney General for Human Resources and Administration. In an April 30, 2012, memorandum, the Deputy Assistant Attorney General requested that the BOP provide an implementation plan, which the BOP submitted on June 1, 2012, showing that the BOP could be brought into compliance with its delegated authority by August 2012.

In addition, on June 13, 2012, BOP and SEPS personnel met to discuss a JSTARS deployment strategy for the BOP. BOP personnel stated they would make their deployment decision by the end of June 2012. SEPS stated that the BOP's use of JSTARS will ensure pre-employment waivers are reviewed by BOP security staff before employees and contractors commence work.

OIG Analysis: SEPS's actions are responsive to our recommendation. Please provide a copy of the BOP's implementation plan by October 15, 2012, that reflects procedures to ensure all pre-employment waivers are completed according to the appropriate delegation authority.

Recommendation 11: The components develop and implement procedures to ensure field offices have access to headquarters' security information.

and

Recommendation 12: The components require each field office to know the type of clearance each employee holds on site.

Status: Resolved.

SEPS Response: SEPS concurred with Recommendations 11 and 12 in a single response. SEPS stated that it believed the recommendations could be implemented if all components provide their field offices access to JSTARS or provide them with monthly reports, a practice SEPS has recommended the practice to all components. To date, only the Executive Office for U.S. Attorneys has chosen to use this functionality in JSTARS. The Department Security Officer will remind all Security Programs Managers of this functionality by August 1, 2012, and request that they share information with their respective field offices.

OIG Analysis: SEPS's planned actions are responsive to our recommendation. Please provide documentation indicating that SEPS has notified components about the specific information access functionality of JSTARS by October 15, 2012.

Recommendation 13: The Department require components to track and report reciprocity data.

Status: Resolved.

SEPS Response: SEPS concurred with this recommendation. SEPS stated that JSTARS was built with this functionality and that the components will be compliant when the system is utilized. SEPS has been able to track this information since the system's inception on July 21, 2008.

OIG Analysis: SEPS's actions are responsive to our recommendation. Please provide documentation that each component is compliant with JSTARS reciprocity tracking requirements by April 15, 2013.

APPENDIX XXI: THE OFFICE OF ATTORNEY RECRUITMENT AND MANAGEMENT RESPONSE TO DRAFT REPORT



U.S. Department of Justice

Office of Attorney Recruitment and Management

Washington, D.C. 20530

July 2, 2012

TO: Office of the Inspector General
Evaluation and Inspections Division

FROM: 
Louis DePalaise
Director
Office of Attorney Recruitment and Management (OARM)

SUBJECT: The Office of the Inspector General's Draft of a Review
Of the Department's and Components' Personnel Security Processes

By EMAIL dated June 20, 2012, the Office of the Inspector General (OIG) requested this office offer comments on the OIG's draft report titled, "The Department's and Components' Personnel Security Processes"(Draft). The Office of Attorney Recruitment and Management (OARM) has reviewed the Draft and provides the following comments.

Background

Under DOJ order 2610.2B, Department Human Resources Offices have delegated authority to make suitability determinations for non-attorney employees pursuant to 5 CFR 731, which sets forth the standards and process for suitability determinations for the competitive service, career Senior Executive Service positions, and those excepted service positions in which "... the incumbent can be noncompetitively converted to the competitive service." 5 CFR 731.101. DOJ 2610.2B specifies that suitability determinations for attorneys and law clerks will be made by OARM. National Security determinations are vested in the Department's Security Officer, here the Director of the Security and Emergency Planning Staff (SEPS). DOJ 2610.2B 7. OARM will therefore offer comments only on those aspects of the Draft that touch on attorney/law student suitability determinations and defer to SEPS on all matters relating to National Security determinations.

It is important to note that approximately half of the Department's career attorney appointments are made under Title 28 authority as opposed to Title 5 authority, and that those appointed under Title 5 authority are not appointed subject to noncompetitive conversion to the competitive service. Thus, while the suitability review for career Department attorneys is, in large part, based on similar factors and processes as those set out in 5 CFR 731, it is more broad and in depth given the nature and scope of the work of the Department's attorneys. Application of distinctive criteria for attorney suitability review is consistent with distinctions made in the appropriations laws with respect to attorneys. In addition to the exclusions generally applicable to excepted service hires, appropriation laws exempt attorney hires from outside rating and examination processes otherwise applicable to government employment.

It is also important to note why it is appropriate and necessary to give a very high level of scrutiny to the suitability of attorney applicants. Line attorneys exercise discretion that can profoundly impact the life, liberty and property of citizens. Every issue noted in the standard suitability requirements is thoroughly vetted. In fairness, candidates are also given the opportunity to respond to such issues, all of which takes time.

For your convenience, the following OARM comments are grouped by topic: BI adjudication time, two anecdotal examples, changing the security clearance process for greater efficiency, and recommendations.

BI Adjudication Time

Page 29 of the Draft states that from October 1, 2009 to December 31, 2010, OARM received over 1000 completed background investigations, and completed only 234 adjudications. This is accurate under the parameters set out for your study as only 234 cases were approved by OARM and SEPS out of the 1,000 received during that same time period.

However, for clarity and background, OARM's data, obtained from reports run on the JSTARS system and an additional database (which stored information on cases initiated prior to the implementation of JSTARS), reflects that during this time period OARM received 1024 BIs and adjudicated 748 BIs. (Reports reflecting these figures were previously provided as Attachments A, B and C to OARM's January 26, 1012 comments.) Two factors may account for the difference between 234 cases and 748: (1) OARM's approvals of cases previously pending (BIs initiated prior to 10/1/09) and (2) cases reviewed for suitability by OARM, but not by SEPS for National Security.

OARM also notes that BIs conducted by the FBI, which are mandated for attorneys under the Department's Security Order, DOJ 2610.2B, are typically lengthier and provide more detailed information than those conducted by other agencies; accordingly, they require more time to review than those used for other employees. Additionally, a few components have asked to routinely review the BIs of their attorneys after OARM reviews the file, and before SEPS completes its review, which adds to the total adjudication time.

Two anecdotal examples

The draft report discussed two cases in which excessive processing delays were cited. This is correct and it was discovered to involve human error and corrective steps have been implemented. However, in most instances, any delay in completing suitability review is caused by the need to resolve questions and issues that arise in individual cases and based on the concerns expressed in your report even though, as you note, your focus is the national security timeliness and not suitability timeliness as such. To help shorten the turnaround time we have changed our internal order of reading and addressing the BI's. OARM had been operating on a priority based on the employee's entry on duty (EOD) date irrespective of the receipt date of the BI. We now read them in the order of receipt which should help SEPS meet the IRPTA timeliness deadlines, for as long as OARM continues to act first. If we are able to reverse the order of consideration (as

discussed below) the timeliness problem in meeting security time standards should be substantially solved.

Changing the Security Clearance Process for Greater Efficiency

The Draft suggests that OARM consider the possible benefits of an attorney process similar to the EOUSA non-attorney system or the FBI system. The EOUSA system cannot be adopted as it would be contrary to DOJ order 2610.2B's requirement that OARM perform the suitability approval on all Department career attorneys and therefore OARM cannot delegate any portion of this function to SEPS. However, the FBI model may in fact be a viable option. Implementing this option presents a technological and budget issue as the JSTARS tracking system would have to be redesigned to allow this. SEPS is pursuing those issues. If this is done it should substantially shorten the time for National Security Clearances of Department attorneys.

Recommendations

The draft report makes 4 recommendations on page 37. The recommendations, and OARM's comments with respect to each, are set forth below.

1. OARM work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRPTA timeliness goals.

As discussed above OARM is working with and supporting SEPS in developing a process whereby SEPS conducts its review and approval of investigations prior to OARM's suitability adjudication. This change in process would allow SEPS to obtain attorney BIs immediately upon their completion, and to conduct their review within the IRPTA time frames. As noted in the draft report, OARM's suitability adjudication is not subject to IRPTA guidelines.

As noted above, implementation of a reversal of BI review order will require a significant revision of the current workflow process in the electronic tracking system (JSTARS). A meeting has been scheduled on July 10, 2012, for representatives from SEPS, OARM and JSTARS to discuss the necessary revisions. It is OARM's understanding that the time frame for implementation of the required changes to JSTARS is dependent upon funds availability. As the Manager of JSTARS, SEPS may be able to provide additional information regarding budget constraints and anticipated timeframes.

2. OARM reduce the time-limited appointment waiver period from 18 months to 12 months and 1 day to complete suitability determinations.

OARM concurs with the recommendation to reduce the initial time-limited appointment and notes that effective 4/8/12, the initial appointment was changed to 14 months. Although OARM considered the 12 month 1 day appointment we feel the 14 month change to be more desirable in order to be consistent with 5 CFR 213.3102(e). This is the maximum period that can be allowed to law clerks (graduating law students hired under the Honors Program) to complete their bar admission requirement. As opportunities to take the bar exam are limited, it is desirable to keep

the 14 month standard for entry level appointments. By shortening the time limited initial appointment to 14 months we keep parity between the entry level attorney appointments and those for lateral attorneys. Also, before the switch to 18 months the standard had been 14 months and is still familiar to the components. In addition, other than its effect on employee benefits and bar admission opportunity, the exact time period of such an appointment has no practical impact as we are now reading BIs in order of receipt. BIs without issues will be disposed of in advance of either a 12 month 1 day limit or a 14 month limit. Likewise, if an extension is required to resolve issues, the difference in the two time limits has little practical effect. Some period must be chosen for time limited appointments but whether 18 months, 14 months, or 12 months and a day, it has no bearing on the time it takes to finish processing an approval. Many cases will be disposed of in less time and the rest will result in extension until resolution of all issues or rejection.

3. OARM increase the amount of staff dedicated to processing completed investigations.

Although additional resources can in most circumstances speed any process, both Department wide and office specific circumstances make it unlikely that additional help will be available in the short run. However, the same circumstances have also substantially reduced the pool of BIs awaiting initial reading and processing. Any portion of delay attributable to the ratio of new work to available personnel has been so reduced that the allocation of additional resources to BI review would not significantly expedite the review process at this time. This would of course change with a return to former hiring levels.

4. SEPS work with OPM, FBI and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's timeliness reports.

As noted above and by your report (FN 41), OARM's suitability adjudications are not subject to IRPTA guidelines, but OARM will actively cooperate with and assist SEPS with their IRPTA reporting responsibility in any way feasible.

Thank you for the opportunity to provide these comments and to work with you to improve operational processing.

APPENDIX XXII: OIG ANALYSIS OF THE OFFICE OF ATTORNEY RECRUITMENT AND MANAGEMENT RESPONSE

The Office of the Inspector General provided a draft of this report to the Office of Attorney Recruitment and Management for its comment. OARM's response is included in Appendix XXI to this report. The OIG's analysis of OARM's response and the actions necessary to close the recommendations are discussed below.

GENERAL COMMENTS

OARM provided comments on aspects of the report that related to suitability determinations for attorneys and law students. In particular, OARM discussed the adjudication times, two examples mentioned in the report, and changing the security clearance process review for non-FBI attorneys.

Although OARM's response acknowledges the accuracy of our finding that OARM completed only 234 attorney security adjudications out of the more than 1000 background investigations received during our review period, the response nevertheless takes issue with this finding, asserting that the report data did not include all of the cases OARM processed for suitability adjudication during the review period. OARM believes that the proper number of attorney security adjudications it completed is 748.

As for our finding of 234 completed attorney security adjudications, we note that our data was provided to us by OARM from JSTARS, and at our request, the data included only those cases for which both the background investigation and the adjudication were completed during our review period. Our methodology, which is disclosed in our report, ensured that we were assessing the end-to-end security clearance process for Department employees. To this end, we only examined OARM's role in completing suitability reviews in so far as it resulted in significant delays to the security clearance process for non-FBI attorneys. We therefore did not include a separate analysis of all of OARM's suitability determinations during this period, and we did not assess the number of background investigations adjudicated by OARM during the review period that were already pending at the beginning of the review period. These additional analyses would not have provided useful insights into the frequency, extent, or causes of delays in the end-to-end security clearance process for Department employees.

At OARM's request, and to ensure the accuracy of our report, the OIG verified its data with SEPS and conducted additional analyses of data from both JSTARS and OARM's internal system in an attempt to verify OARM's assertion that it completed 748 adjudications during the review period. We were unable to do so. Nor did we receive evidence that OARM had reviewed a significant number of attorney cases for suitability during the review period that were still pending a security review by SEPS, as OARM asserts in its response.

OARM's response also expresses concern about two cases highlighted in our report for excessive delays caused by human error. The response states, "[I]n most instances, any delay in completing suitability review is caused by the need to resolve questions and issues that arise in individual cases" However, the OIG reviewed the security files for an additional 10 attorney cases representing the two longest attorney cases for each quarter in FY 2010 and the first quarter of FY 2011, and we found that only two of these cases contained questions and issues relating to derogatory information that could possibly explain the length of the security process. This sample of 10 files was inadequate to reach a broad conclusion about the most common cause of delays in completing security clearance adjudications, yet it also offered no support to the assertion in the OARM's response.

RESPONSES TO RECOMMENDATIONS

Recommendation 1: OARM work with SEPS to develop and implement a process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals.

Status: Resolved.

OARM Response: OARM concurred with this recommendation. OARM stated that was working with and supporting SEPS in developing a process whereby SEPS conducts its review and approval of investigations prior to OARM's suitability adjudication. This change in process would allow SEPS to obtain attorney background investigations immediately upon their completion and to conduct its review within the IRPTA time frames. As noted in the draft report, OARM's suitability adjudication is not subject to IRPTA guidelines.

Implementing a reversal of the background investigation review order will require a significant revision of the current workflow process in JSTARS. A meeting was scheduled for July 10, 2012, for representatives from SEPS, OARM, and JSTARS to discuss the necessary revisions. It

was OARM's understanding that the time frame for implementing the required changes to JSTARS depended on the availability of funds.

OIG Analysis: The actions taken by OARM are responsive to our recommendation. By October 15, 2012, please provide a status report regarding the meeting with SEPS and documentation showing how OARM and SEPS have revised the process for reviewing and adjudicating non-FBI attorney investigations to meet the IRTPA timeliness goals.

Recommendation 2: OARM reduce the time-limited appointment waiver period from 18 months to 12 months and 1 day to complete suitability determinations.

Status: Resolved.

OARM Response: OARM concurred with the recommendation to reduce the initial time-limited appointment. OARM noted that effective April 8, 2012, the initial appointment was changed to 14 months. Although OARM considered the 12 month 1 day appointment, it believed the 14-month change to be more desirable in order to be consistent with 5 C.F.R. 213.3102(e). It is the maximum period that can be allowed to law clerks (graduating law students hired under the Honors Program) to complete their bar admission requirement. As opportunities to take the bar exam are limited, it is desirable to keep the 14-month standard for entry-level appointments. Shortening the time-limited initial appointment to 14 months keeps parity between the entry-level attorney appointments and those for lateral attorneys. Also, before the switch to 18 months, the standard had been 14 months and is still familiar to the components. OARM also stated that other than its effect on employee benefits and bar admission opportunity, the exact time period of such an appointment has no practical impact as it is now reading background investigations in order of receipt. OARM stated that it will dispose of background investigations without issues before either a 12-month-1-day or a 14-month limit is reached. If an extension is required to resolve issues, the difference in the two time limits has little practical effect, according to OARM. It stated that many cases will be disposed of in less time and that the rest will result in extensions until all issues are resolved or the employee is rejected.

OIG Analysis: OARM's actions are responsive to this recommendation. Please provide a copy of the April 8, 2012, decision to change the initial appointment period from 18 months to 14 months by October 15, 2012. Please provide documentation reflecting the number and percentage of approvals completed within the 14 month time frame by April 15, 2013.

Recommendation 3: OARM increase the amount of staff dedicated to processing completed investigations.

Status: Resolved.

OARM Response: OARM concurred with this recommendation. OARM stated that given Department-wide and office-specific circumstances, it was unlikely that additional staff will be available in the short run. However, the same circumstances have also substantially reduced the pool of background investigations awaiting initial reading and processing. Any portion of delay attributable to the ratio of new work to available personnel has been so reduced, according to OARM, that the allocation of additional resources to background investigation review would not significantly expedite the review process at this time. OARM noted that this would of course change with a return to former hiring levels.

OIG Analysis: OARM's actions are responsive to this recommendation. However, we believe that until OARM addresses its staffing and work process issues, suitability reviews for attorneys will continue to be subject to significant delays, particularly when there is a high volume of new hires. Please develop a plan for re-allocating OARM's staff and work processes and provide a copy to the OIG by October 15, 2012, and verify that the plan is current every 6 months until the recommendation is closed.

Recommendation 4: SEPS work with OPM, FBI, and OARM to ensure that all of the attorney background investigation and adjudication data is included in the Department's IRTPA timeliness reports.

Status: Closed.

OARM Response: OARM concurred with this recommendation. OARM stated that as the OIG's report noted, suitability adjudications are not subject to IRPTA guidelines, but stated that OARM will actively cooperate with and assist SEPS with its IRPTA reporting responsibility in any way feasible.

OIG Analysis: In response to our recommendation, which was directed to SEPS, the OARM agreed to work with SEPS to meet its IRTPA reporting responsibility for non-FBI attorneys. No further status reports are required from the OARM on Recommendation 4.